##

Input to the UN General Comment on children’s rights in relation to the digital environment

**November 2020**

PICUM is a network of 167 organisations that has worked for nearly twenty years to advance the rights and improve the situation of people who are undocumented across a variety of areas, including access to health care, access to justice, the rights of undocumented workers, labour migration, the rights of children, families and youth, as well as fundamental rights in the context of immigration detention and return.

We appreciate the opportunity to provide input on the draft [General Comment no. 25](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en) to the UN Committee on the Rights of the Child.

[I. Background 2](#_Toc56509407)

[Trends in National-Level Policy and Practice in Europe 2](#_Toc56509408)

[Trends in EU Policy 3](#_Toc56509409)

[II. Suggested Revisions to the text of the Draft General Comment 4](#_Toc56509410)

[Resources 7](#_Toc56509411)

# Background

For all its benefits, the increased use of digital technology can drive increased discrimination against and exclusion of some groups. For people with irregular migration status, the state’s use of technology and processing of personal data is typically to support immigration enforcement actions and entails the policing of otherwise normal behaviours of people often belonging to communities of colour to detect whether they are present without authorisation.

## Trends in National-Level Policy and Practice in Europe

In Europe, despite [strong regulations](https://ec.europa.eu/info/law/law-topic/data-protection_en) governing the processing of personal data, personal data is widely shared in the context of **undocumented people trying to report crime or mistreatment to the police**. For instance:

* In Belgium, the [police have a duty](file:///C%3A/Users/asmith/AppData/Local/Microsoft/Windows/Temporary%20Internet%20Files/Content.Outlook/MCBLEDHM/pdf) to report victims of crime with irregular status to the Immigration Office. In some cases, police precincts adopt a practice of wilful ignorance, declining to inquire about a person’s residence status, and thus to report. The Immigration Office also retains the discretion not to prosecute people for immigration offences. However, undocumented people are left with significant uncertainty about whether coming forward to engage with law enforcement, including as victims of crime, will result in their deportation in any given case.
* In the United Kingdom, the National Police Chiefs’ Council adopted a [revised policy](https://news.npcc.police.uk/releases/new-guidance-for-officers-on-sharing-information-with-immigration-enforcement) in 2018 declaring their prioritisation of victims’ rights ahead of immigration enforcement - but reserving the right to share data with the immigration service, if they became aware of it. The intention of the policy is to promote confidence in the police; however, by preserving the right to share immigration information with the Home Office, they undermine that very confidence because people coming forward cannot know if their immigration status will be shared, should it become known, and if so what the Home Office’s response will be.

Personal data is also used to “police” people who are undocumented when they **access health care, social services, and education**. In addition to undermining their economic and social rights, their rights to due process and to the protection of their privacy and personal data, in practice this also leads to racial profiling and discrimination.

* In Germany, undocumented people have the same right to health care as asylum seekers under the Asylum Seekers Benefit Act – but the social welfare office that mediates their right to care [must share their data with immigration authorities](https://www.diakonie.de/fileadmin/user_upload/Diakonie/PDFs/Broschuere_PDF/English_Version_BAG_Gesundheit_Illegalitaet_Arbeitspapier_Gesundheitsversorgung_fu__r_Menschen_ohne_Papiere_April_2017.pdf), under section 87 of the Residence Act, which governs the “transfer of data and information for foreign authorities” by all public authorities.
* In the United Kingdom, [charging for secondary health care](https://www.gov.uk/guidance/nhs-entitlements-migrant-health-guide) has been introduced for undocumented people and others without “ordinary residence”. People with irregular status are therefore billed 150% of the cost of secondary care to the National Health Service (NHS). If a patient is unable to pay their debts to the NHS, the Home Office is automatically informed, which may have consequences for their ability to later renew or apply for a residence permit. In April 2020, the UK government [updated](https://www.gov.uk/guidance/nhs-entitlements-migrant-health-guide) its regulations to include COVID-19 in the list of conditions exempted from charges for migration. However, advocates are concerned that the guidance leaves doubt about undocumented people and provides no definitive assurance of a “firewall” between the NHS and the Home Office. A 2019 report revealed that an NHS trust shared patients’ data with the financial firm Experian so that it could check their economic activities and determine which overseas visitors or migrants could be charted for health care. The [NHS contacted](http://7z96.mjt.lu/lnk/AMMAAFLSJpEAAchhAiIAALF9GpoAAAAy4S0AAAAAAArq4ABdwUHgc3E7BJbYS-qOWpmLzRkb4QAK13g/63/V8jmKanict9IZkQr5_Dwdw/aHR0cHM6Ly9waWN1bS5vcmcvd3AtY29udGVudC9wbHVnaW5zL2Npdmljcm0vY2l2aWNybS9leHRlcm4vdXJsLnBocD91PTg0NCZxaWQ9MjEzMzM) an additional 51 trusts to carry out similar check.
* It has also been reported that social media monitoring is being conducted by [local governments](https://edri.org/our-work/uk-stop-social-media-monitoring-by-local-authorities/) in the UK for the purpose of investigation before issuance of, for example, benefits, debt recovery, fraud and children’s social care. For some families this means that life-changing decisions will be made based on their online appearance, without their knowledge, while the effectiveness of this form of surveillance on decision-making is unknown.

The routine nature of privacy breaches against migrants is illustrated in the case of Germany, where the Federal Office for Migration and Refugees systematically examines data from the mobile phone of people who present with a valid passport, upon arrival in the country – without any individualised reason for suspicion – to verify information provided about their identity. The extraction from mobile devises has no age limit, allowing the data on children’s phones to be analysed as well for this purpose. This highly invasive practice has been documented in a [report](https://freiheitsrechte.org/study-invading-refugees-phones/) that ultimately laid the groundwork for litigation launched against the Germany government in May 2020 by Berlin-based digital rights defenders, Gesellschaft für Freiheitsrechte.

## Trends in EU Policy

Similar trends are evident at the EU level:

* ***Interoperable migration databases:*** In 2019, the EU enacted two regulations that massively scale up the potential use of immigration data systems (together with data on criminal records) to pursue immigration enforcement *and* serious crimes. These regulations provide a legal foundation for the creation of a new layer of architecture on top of existing migration databases, to permit interoperability: that is, to allow the underlying databases to be interconnected in a way that purportedly supports more efficient law and immigration enforcement. PICUM partnered with Statewatch to produce a [report](https://picum.org/wp-content/uploads/2019/11/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf) setting out the implications of interoperability for undocumented people. This interoperability framework has [raised](https://picum.org/wp-content/uploads/2020/04/INFOGRAPHIC.-Interoperability-Systems-and-Access-to-Data_WEB_RGB.pdf) concerns for being highly discriminatory in that it only targets non-EU nationals (i.e., foreigners) for purposes that co-mingle immigration enforcement and the targeting of “serious crimes” like terrorism, implying a false link between criminality and immigration. It also creates a deeply complex system with multiple interconnecting databases. This technical complexity only increases the likelihood of errors and makes it extremely difficult to inform people about how their data is used, how they can rectify their data and obtain effective remedies in the event of errors or abuses. Lawyers, data protection authorities and others essential to safeguarding the rights of the millions of people whose data is concerned are still struggling to understand the new systems and what they mean for people’s rights.
* ***Facial recognition and immigration enforcement:*** The European Commission recognised in its [White Paper on AI](https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf) that the “gathering and use of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks for fundamental rights”. According to a [study](https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software) from the U.S. National Institute of Standards and Technology (NIST), facial recognition systems tend to lead to remarkably higher rates of false positives among people of colour. And yet, according to [European Data Rights (EDRI)](https://edri.org/tag/ai-white-paper/), “at least 15 European countries have experimented with highly intrusive facial and biometric recognition systems for mass surveillance.”

Despite calls by civil society for a moratorium until there has been adequate public debate and proper assessment of risks and needed safeguards to preserve fundamental rights, there have been [reports](https://theintercept.com/2020/02/21/eu-facial-recognition-database/) that the EU plans to establish an EU-wide network of facial recognition databases. European police already have access to databases with fingerprints and DNA across the EU and, in some cases, the United States through the [Prüm system](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU%282018%29604971_EN.pdf). A [2019 report](https://theintercept.com/2020/02/21/eu-facial-recognition-database/) by national police forces in 10 EU countries, led by Austria, urges new legislation to expand Prüm to create and interconnect national police facial recognition databases in every member state. The European Commission [commissioned or funded studies](https://digit.site36.net/2019/07/22/european-union-plans-borderless-query-of-facial-images/), totalling more than 1M €, on possible changes to the Prüm system, including facial recognition technology.

Significantly, the European Commission has indicated that: “Provided that the necessity will be demonstrated, decentralised systems such as those operated under the Prüm framework, the Passenger Name Record (PNR) Directive and the Advance Passenger Information Directive may at a later stage be linked up to one or more of the [interoperability] components.”[[1]](#footnote-1)

# Suggested Revisions to the text of the Draft General Comment

***PICUM proposes the following adapted or new wording in bold in the paragraphs below and highlighted in yellow***

**The Right to Privacy (art. 16)**

1. Digital technologies are used to collect data about, inter alia, children’s identities, activities, location, communication, preferences and relationships. Children’s personal data are often processed to offer educational, health and other benefits to children. Certain combinations of personal data, including biometric data can be used to uniquely identify a child. Digital practices such as automated data processing, behavioural targeting, mandatory identity verification, and mass surveillance are becoming routine. **Digital tools, and in particular mass surveillance and large-scale processing of personal data, may be applied in ways that reinforce existing forms of discrimination, especially when intended to support law and immigration enforcement purposes.** Such practices may lead to arbitrary or unlawful interference with children’s right to privacy**, or with the right to privacy of a parent or guardian, which can have a significant negative impact on the child**; they are rarely transparent to children or their parents or caregivers, and may have adverse consequences on children, which may extend to later stages of their lives. Children are concerned about their privacy and want to better understand how their data is collected and used.
2. **States’ obligations with respect to a child’s right to privacy are not limited to a state’s citizens but apply with respect to everyone on a state’s territory, regardless of residence or migration status.** Interference with a child’s privacy is only permissible if it is neither arbitrary nor unlawful (article 16). This means any such interference must be provided for by law, be aimed at achieving a legitimate purpose, be proportional and not in conflict with the provisions, aims and objectives of the Convention.
3. States shall take legislative and other measures to ensure that children’s privacy is respected and protected by all organizations and in all environments that process their data**, with particular attention to the rights of children at greatest risk of discrimination, such as those from economically disadvantaged backgrounds; racial, ethnic or religious minorities; or migrants, especially those with irregular status**. Such legislation should include strong safeguards, independent oversight and access to remedy. **It should also require transparency regarding any agreements between state and privacy companies regarding the use of digital technologies to do large-scale processing or surveillance of individuals.** States should encourage the adoption of privacy-by-design, such as end to end encryption, in services that impact on children. States should regularly review such legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children’s privacy. States should ensure that consent to process a child’s data is informed and freely given by the child or, depending on the child’s age and maturity, by the parent or caregiver, and obtained prior to the processing.

***Proposed new paragraph*:**

**States should, at the national, regional and local levels, establish mechanisms that ensure careful review of the implications for at-risk groups of the use of technology; and develop clear guidelines about the use of personal data and algorithms, based on meaningful input from and engagement with relevant stakeholders including digital rights organisations, representatives from affected communities, non-governmental organisations, data protection authorities, and equality bodies. These guidelines should address data-driven profiling as a form of discrimination incompatible with fundamental rights; and clarify the strict standards for derogations.[[2]](#footnote-2) States should support and strengthen national equality bodies, data protection authorities, and other relevant public bodies to enhance their capacities to ensure accountability for the implications of digital technology and data processing for human rights and discrimination; and support non-governmental organisations’ increased and active engagement in the area of digital rights, particularly among organisations with deep knowledge of and experience with issues of migration, discrimination and inequality, but that may not have a long history of working on issues of technology.**

**Protection of Children in Armed Conflict, Migration and Other Vulnerable Situations (arts 22 and 38; OPAC)**

1. The digital environment can provide children living in vulnerable situations, including children in armed conflict, internally displaced children, migrant, asylum-seeking and refugee children, unaccompanied children, children in street situations and children affected by natural disasters, with access to life-saving information vital for their protection. The digital environment can also enable them, where necessary, to maintain contact with their families; to access education, health and other basic services; as well as obtain food and safe shelter. States should ensure the safe and beneficial access of children to the digital environment, and ensure their protection from violence, exploitation and abuse.

***Proposed new paragraph*:**

**The use of digital tools, including mass surveillance and the large-scale processing of data, can aggravate existing inequalities and discrimination experienced by children and families living in vulnerable situations. This includes the use of algorithm and facial recognition digital technology in policing, with its disparate impact based on race or ethnicity; and the growing use of digital technology to support migration enforcement at a state’s borders and within its territory. Such uses of technology can have a harmful impact on children, by increasing the likelihood that they and their families will experience unlawful profiling and discrimination.]**

1. States should ensure that children are not recruited or used in conflicts, including armed conflicts, through the digital environment. This includes preventing, criminalizing and sanctioning different forms of online solicitation of children, for example through social networks or chat services in online games. **States should also ensure that digital technologies are not deployed in ways that increase the risk of discrimination against children and families living in vulnerable situations.**

# Resources

ENAR (2019), [Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe](https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf)

European Commission against Racism and Intolerance (ECRI), 16 March 2016, [ECRI General Policy Recommendation No. 16 on Safeguarding Irregularly Present Migrants From Discrimination](https://rm.coe.int/ecri-general-policy-recommendation-no-16-on-safeguarding-irregularly-p/16808b5b0b).

Francois Crépeau, “[The Case for “Firewall” Protections for Irregular Migrants: Safeguarding Fundamental Rights](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2780641)”, 17 May 2016, *2-3 European Journal of Migration and Law* 157-183.

Molnar P., 12 February 2020, “[The human rights impacts of migration control technologies](https://edri.org/the-human-rights-impacts-of-migration-control-technologies/)”.

PICUM (2020), “[How do the new EU regulations on interoperability lead to discriminatory policing](https://picum.org/wp-content/uploads/2020/04/INFOGRAPHIC.-Interoperability-Systems-and-Access-to-Data_WEB_RGB.pdf)?”

Statewatch, (2019) “[Data Protection, Immigration Enforcement and Fundamental Rights: What the EU’s Regulations on Interoperability Mean for People with Irregular Status](https://picum.org/wp-content/uploads/2019/11/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf)”.

UN Committee on Economic, Social and Cultural Rights, 13 March 2017. [Duties of States towards refugees and migrants under the International Covenant on Economic, Social and Cultural Rights – Statement by the Committee on Economic, Social and Cultural Rights](http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=4slQ6QSmlBEDzFEovLCuW1AVC1NkPsgUedPlF1vfPMJbFePxX56jVyNBwivepPdlEe4%2BUb4qsdJhuBDpCRSOwCXPjZ7VN7SXN0oRoXkZhCuB9Z73iyU35LZveUjX0d7u), E/C.12/2017/1.

UN Special Rapporteur on contemporary forms of racism, [Report to the 75th session of the General Assembly on border and immigration enforcement](https://www.ohchr.org/EN/Issues/Racism/SRRacism/Pages/SRRacismThematicReports.aspx), A/75/590.

UN Special Rapporteur on contemporary forms of racism, [Report on different forms of racism in the design and use of emerging digital technologies, including the structural and institutional dimensions of discrimination](https://www.ohchr.org/EN/Issues/Racism/SRRacism/Pages/SRRacismThematicReports.aspx), A/HRC/44/57.

1. European Commission, [Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:794:FIN), COM(2017) 794 final, 12 December 2017. [↑](#footnote-ref-1)
2. The EU’s Draft Ethics Guidelines for Trustworthy AI underscore how the use of AI can lead to discrimination, through data bias, incompleteness and bad governance. The Council of Europe’s Commissioner for Human Rights has issued recommendations on how to mitigate the “discrimination risks” of AI systems, including through consultation with diverse communities. Council of Europe Commissioner for Human Rights (May 2019), [Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights](https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights).  [↑](#footnote-ref-2)