Privacy International's response to the call for input to a report on the right to privacy in the digital age by the UN High Commissioner for human rights

June 2022

Introduction

Privacy International (PI) welcomes the opportunity to provide input to the report of the UN High Commissioner for Human Rights (HCHR) on the right to privacy in the digital age. We believe that this forthcoming report could reflect on the developments that have taken place since 2018 and to assess the extent that states, companies, and other actors have implemented the recommendations contained in previous HCHR reports on the right to privacy in the digital age, as well as recommendations and findings of other relevant UN human rights experts and bodies.

The following sections provide PI's information and analysis of some of the topics listed in the call for submission.[1]

1. Targeted and mass surveillance, including of journalists and human rights defenders

1.1 Mass surveillance

In the absence of internationally agreed definition, PI holds that "targeted" surveillance is surveillance in circumstances where there is reasonable suspicion that a specific target has committed or is likely to commit a criminal offence or is engaging in acts amounting to a threat to national security. Conversely, mass surveillance is surveillance that is not 'targeted', using systems or technologies, such as interception of information, that collect, analyse, and/or generate data on indefinite or large numbers of people instead of limiting surveillance to individuals about which there is reasonable suspicion of wrongdoing or whom are not of any legitimate interest to the security and intelligence agencies.[2]

Governments continue to rely on mass surveillance, often justifying it on national security grounds. PI believes that mass surveillance threatens the essence of the right to privacy and fails to comply with the principles of necessity and proportionality. We also note that when challenged before independent

[1] https://www.ohchr.org/en/calls-for-input/calls-input/call-inputs-report-right-privacy-digital-age-2022
[2] https://privacyinternational.org/learn/mass-surveillance

courts, mass surveillance programmes have been found in breach of the right to privacy and other human rights.

PI has been involved in some of these legal challenges. Most notably:

- on 4 February 2021, the Constitutional Court of South Africa declared that bulk interception by the South African National Communications Centre is unlawful and invalid;[3]

- on 25 May 2021, the Grand Chamber of the ECtHR confirmed that the UK mass surveillance laws breached the rights to privacy and freedom of expression.[4] Following this case, the UK government settled a separate claim with two applicants (Human Rights Watch and a journalist), acknowledging that the UK previous investigatory powers regime was not compliant with Article 8 of the European Convention on Human Rights, and in relation to the treatment of confidential journalistic material, Article 10 of the Convention.[5]

1.2 Government hacking

Further, certain surveillance methods that governments proclaim to be 'targeted' result to violations of the right to privacy of individuals, as well as other human rights.

This is notably the case with regards to government hacking. Hacking has been used to target human rights defenders, journalists, and political opponents in ways that violate their human rights, as most prominently revealed in the Pegasus/NSO cases.[6]

Government hacking is unlike any other form of existing surveillance technique. Government hacking can be far more privacy intrusive than any other surveillance technique, permitting to remotely and secretly access personal devices and the data stored on them as well as to conduct novel forms of real-time surveillance, for example, by turning on microphones, cameras, or GPS-based locator technology. Hacking also allows governments to manipulate data on devices, including corrupting, planting or deleting data, or recovering data that has been deleted, all while erasing any trace of the intrusion.

It not only poses unique privacy interference to the intended targets, but it often affects the privacy and security of others in unpredictable ways. Hacking is about causing technologies to act in a manner the manufacturer, owner or user did not intend or did not foresee. It often depends on exploiting vulnerabilities in systems to facilitate surveillance objectives. It is therefore fundamentally at cross-

[3] https://privacyinternational.org/legal-case-files/4415/amabhungane-case-constitutional-court-judgment
[4] For PI's legal analysis of this judgement: https://privacyinternational.org/long-read/4526/uk-mass-interception-laws-violates-human-rights-and-fight-continues
[5] https://privacyinternational.org/news-analysis/4818/uk-government-acknowledges-past-violations-individuals-rights-and-fight
[6] https://www.privacyinternational.org/press-release/4596/press-note-release-report-operating-shadows-inside-nso-groups-corporate

purposes with digital security aims: in the surveillance context, the government identifies vulnerabilities, not to secure systems through testing and coordinated disclosure, but to exploit them in order to facilitate a surveillance objective. This approach only undermines the security of the target system but also of other systems.[7]

1.3 Mobile phone extraction

Mobile phone extraction tools enable police and other authorities to download content and associated data from people's phones. This can apply to suspects, witnesses, and even victims of crime – often without their knowledge or consent.[8]

The risks that this surveillance technology poses are well illustrated in the case brought by asylum seeking claimants in the UK, which resulted in a High Court ruling on 25 March 2022 that the UK government acted unlawfully and breached human rights and data protection laws by operating a secret, blanket policy of seizing, retaining and extracting data from the mobile phones of asylum seekers arriving by small boats.[9]

Increasingly mobile phone extraction can be used to target protestors without an appropriate legal framework or safeguards.[10] Human rights groups have warned about use of such intrusive technologies in Argentina, Colombia, Palestine, Paraguay, and the UK.[11] Other countries are reportedly using such capabilities in violation of human rights standards, including Argentina.[12]

1.4 Examples of surveillance targeting human rights defenders

Because of its covert nature, lack of authorisation or oversight, and the lack of notification mechanisms, it is notoriously difficult to document examples of surveillance of individuals. Surveillance that is often conducted without a legitimate justification, such as ongoing criminal investigation. However, such instances are increasingly documented, as for example with Pegasus/NSO cases above. Moreover, PI has collected testimonies of human rights defenders in Colombia, Indonesia, Mexico, and South Africa.[13]

---

[7] For PI's safeguards on government hacking: https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf.

[8] https://privacyinternational.org/long-read/3256/technical-look-phone-extraction

[9] https://privacyinternational.org/press-release/4812/press-release-high-court-rules-seizing-and-retaining-mobile-phones-asylum

[10] https://privacyinternational.org/explainer/4484/how-mobile-phone-extraction-can-be-used-protest

[11] See the guides produced by groups from each country: https://privacyinternational.org/campaigns/freetoprotest

[12] It has been documented that such surveillance capabilities have been acquired by various security and law enforcement bodies in Argentina including Cellebrite's ''Universal Forensic Extraction Device'' (UFED) by the Argentine National Gendarmerie (GNA) which has 35 licenses to use this tool, the Airport Security Police (PSA) which may have at least licenses, the Argentine Naval Prefecture, various Regional Forensic Investigation Laboratories set up by the Ministry of Justice and Human Rights across the country, as well as various provincial ministerial bodies in Santa Fe, Córdoba, Autonomous City of Buenos Aires, Salta, Chubut, Santiago de Estero, Chaco. Other products and tools documented to have acquired by law enforcement agencies including MSAB's forensic mobile phone tool XRY and Magnet Forensics's Magnet AXIOM. https://adc.org.ar/informes/quien-revisa-tu-telefono/

[13] https://privacyinternational.org/campaigns/being-target

Further in 2021, the Defenders Coalition in Kenya published the results of its survey of 56 human rights defenders from across Kenya, who have raised concerns about their mobile phones being tapped and their communication intercepted. As the report notes, these experiences have had a chilling effect on the exercise of their rights and freedoms of expression, association, and assembly.[14]

1.5 The role of industry

Although it is possible that some governments manufacture tools to conduct digital surveillance themselves, many states buy the sophisticated technology enabling such surveillance from private companies. They justify the procurement of these technologies as essential for maintaining law and order.[15] Some of these surveillance companies manufacture and sell spyware or other such tools to states, who have, in addition to legitimate purposes, used surveillance to shrink the space for dissent by targeting HRDs, in violation of their internationally recognized human rights.[16] These companies are often opaque in their structure, activities and clients. PI together with Amnesty International and SOMO published a briefing to analyse the corporate structure of the NSO group to highlight the human rights risks and corporate dynamics that characterize the broader surveillance industry, and to support civil society in their efforts to seek accountability for abuses.[17] Further, in May 2022 PI reported on the rise of the private intelligence industry where some governments and private actors increasingly resort for conducting surveillance. The report details use of hacking techniques, monitoring of environmental and other activists, and running fake 'astroturfing' campaigns for big polluters and examines the gap in UK current legal regime.[18]

2. Access of state authorities to personal data collected by companies, including in cross-border contexts

2.1 Data retention

Governments continue to impose untargeted, blanket obligations to retain communications data on Telcos and other service providers, despite consistent recognition by courts and human rights experts that these data retention laws and practices breach applicable human rights standards.

In 2020, for instance, the Court of Justice of the European Union (CJEU) issued two judgments ruling that the UK, French, and Belgian bulk data collection or retention regimes must be brought within EU law, confirming that privacy safeguards set out in EU law apply if a national government forces

[14] https://privacyinternational.org/report/4469/defenders-coalition-impact-communication-surveillance-hrds-kenya
[15] See among others PI's Global Surveillance Industry report, 2018, https://privacyinternational.org/explainer/1632/global-surveillance-industry
[16] https://privacyinternational.org/long-read/2852/protecting-civic-spaces
[17] https://www.privacyinternational.org/press-release/4596/press-note-release-report-operating-shadows-inside-nso-groups-corporate
[18] https://www.privacyinternational.org/report/4850/briefing-controlling-uks-private-intelligence-industry For other examples, see https://www.privacyinternational.org/learn/surveillance-industry

telecommunications providers to retain personal data, including when it is done for the purposes of national security.[19]

Regretfully, data retention continues to be in place, including in EU member states which should adhere to the CJEU judgements, and it is only through challenges before national courts that the data retention laws are repealed.[20]

2.2 Public Private Partnerships (PPP) and their implications for the right to privacy

PI and its partners have documented several cases where public authorities (including police forces, but also national and local authorities) partner with private companies in order to expand their surveillance capabilities and process mass quantities of personal data (including often biometric data, such as facial images).[21] These PPPs are taking on a new form, diverging from traditional public procurement relationships. We observe much more co-dependency between the parties, whereby the state may be developing new systems or processes entirely reliant on the services of one company, and the company may be receiving access to data or other information for use in developing its own services.

Examples include:

- Agreement between King's Cross Central Limited Partnership (KCCLP) and the Metropolitan Police for CCTV cameras equipped with FRT in Kings Cross (London, UK);[22]
- Surveillance partnerships between Amazon Ring and law-enforcement around the world;[23]
- Installation of FRT cameras in Como, Italy[24] and Belgrade, Serbia; [25]
- Agreement between Amazon and National Health Service (NHS) in the UK;[26]
- Smart Sustainable cities initiatives in Zimbabwe;[27]
- Installation of CCTV cameras Uganda.[28]

[19] For PI's reaction to the judgments, see https://www.privacyinternational.org/press-release/4205/press-release-ruling-eus-highest-court-finds-uk-french-and-belgian-mass
[20] For example, see https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-04/cp220058en.pdf and https://edri.org/our-work/portugal-constitutional-court-strikes-data-retention-down/
[21] https://privacyinternational.org/learn/public-private-surveillance-partnerships
[22] https://privacyinternational.org/case-study/3973/kings-cross-has-been-watching-you-and-police-helped
[23] https://privacyinternational.org/long-read/3971/one-ring-watch-them-all
[24] https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como
[25] https://privacyinternational.org/case-study/3967/thousands-cameras-citizen-response-mass-biometric-surveillance
[26] https://privacyinternational.org/node/3298; https://www.privacyinternational.org/news-analysis/4486/amazon-alexanhs-contract-ico-allows-partial-disclosure
[27] https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe
[28] https://privacyinternational.org/case-study/3969/huawei-infiltration-uganda

Further, there is a growing reliance by governments on the services offered by data analytics companies, which provide analytical techniques to search, aggregate, and cross-reference large data sets in order to develop intelligence and insights, and thereby inform public decision-making. While per se data analytics tools do not necessarily raise human rights concerns, the way they are used do so. PI has raised concerns about data analytics practices, by companies such as Palantir, whose tools may pose a real danger to people in vulnerable positions such as at international border crossings.[29] PI also documented on the company's contracts with the national health service (NHS) and other critical government departments in the UK.[30] We faced a complete lack of transparency and accountability with regards to the role of Palantir's data analytics in the formulation of public policy – leaving us and the public unable to understand its rationale, nor to challenge any potential underlying human rights abuses.

Based on the United Nations Guiding Principles on Business and Human Rights, PI developed a set of safeguards for states and companies to mitigate the risks of human rights abuses resulting from PPPs that rely on the processing of personal data.[31]

3. Use of publicly accessible information and data by state authorities, for example when monitoring social media

3.1 SOCMINT by government authorities

As noted in the 2018 report of the High Commissioner for Human Rights, "the right to privacy comes into play when a Government is monitoring a public space, such as a marketplace or a train station, thereby observing individuals. Similarly, when information that is publicly available about an individual on social media is collected and analysed, it also implicates the right to privacy. The public sharing of information does not render its substance unprotected."[32]

Social media surveillance is not only the purview of law enforcement and intelligence agencies as already widely documented.[33] In the UK, for example, local authorities are looking at people's social media accounts, such as Facebook, as part of their intelligence gathering and investigation tactics in areas such as council tax payments, children's services, benefits and monitoring protests and demonstrations.[34]

[29] https://privacyinternational.org/long-read/2216/who-supplies-data-analysis-and-tech-infrastructure-us-immigration-authorities
[30] https://privacyinternational.org/report/4271/all-roads-lead-palantir
[31] https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships
[32] https://undocs.org/A/HRC/39/29
[33] https://privacyinternational.org/legal-action/salman-butt-v-united-kingdom and https://privacyinternational.org/sites/default/files/2019-03/Submission%20on%20Article%2021%20of%20ICCPR_0.pdf
[34] https://privacyinternational.org/report/3584/when-local-authorities-arent-your-friends

3.2 Role of private companies

Left unregulated, the routine collection and processing of publicly available information or data may lead to the kind of abuses observed in other forms of covert surveillance operations.

This is particularly so as technologies allow the large scale collection and processing of biometrics data, including facial images. Among the most concerning example of this practice is Clearview, a facial recognition company claiming to have built "the largest known database of 3+ billion facial images". It uses an "automated image scraper" to search the web and collect any images that it detects as containing human faces. All these faces are then run through its proprietary facial software, to build a gigantic biometrics database. Clearview then sells access to this database to private companies and law enforcement authorities. Various actions have been launched across the globe against Clearview's practices, in countries with biometrics or data protection regulation, including by PI.[35]

4. Measures relying on digital technology taken to combat the Covid-19 pandemic

To respond to the challenges posed by the Covid-19 pandemic, governments introduced a range of measures, often relying on untested or poorly tested technologies, including with the aim to track the spread of the virus.[36]

We have observed that the lack of human rights due diligence and effective enforcement of existing human rights obligations and responsibilities of governments and private entities led to short-sighted decision-making with little consideration of what is needed for an effective public health response and limited understanding of the impact on individuals and communities, in particular those in vulnerable positions.[37]

Below we tackle two developments which particularly impacted on the right to privacy, but this is not an exhaustive list of concerns associated with measures deployed during the Covid-19 which had severe implications for people's rights and freedoms.

4.1 Contact tracing and Covid-19 applications

Concerns about the effectiveness of proximity tracing with Bluetooth technologies were coupled with longstanding privacy concerns of using telecommunications data to track individuals.[38] Some countries

[35] https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe See also recent developments in the US https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois
[36] https://privacyinternational.org/campaigns/fighting-global-covid-19-power-grab; https://privacyinternational.org/examples/tracking-global-response-covid-19
[37] https://privacyinternational.org/examples/migration-and-covid-19
[38] https://privacyinternational.org/news-analysis/3461/extraordinary-powers-need-extraordinary-protections. For an outline of different tracking technologies used during the Covid-19 pandemic and their flaws, see PI, Covid-19: a tech post-mortem, https://privacyinternational.org/explainer/4814/covid-2022-tech-retrospective

like Israel attempted, but were prevented from, to use the data generated by such apps to allow the intelligence agency to surveil Covid-19 positive individuals.[39] Reports of repurposing of contact tracing apps for law enforcement goals have emerged in Australia[40], Germany,[41] and Singapore.[42] There were also examples of function creep with contact tracing apps used to enforce lockdown measures and control crowds.[43] Furthermore, organisations around the world documented the lack of privacy safeguards built into the design and implementation of contact tracing apps including in Colombia,[44] the Philippines[45], whilst others reported their disproportionate negative impact on marginalised groups such a women, minority groups and criminalised communities leading to discrimination and stigma.[46]

4.2 Covid-19 vaccination status certification

While it is still too early to assess the effectiveness of Covid-19 vaccination certification, the technical specifications and implementation guidance published by the World Health Organisation on 6 August 2021 offered some important recommendations, particularly around risk and privacy assessments and data protection requirements. As our analysis shows, however, the WHO guidance is remarkably weak in providing technical details to health authorities and makes assumptions on the available national infrastructure which is simply often not there.[47]

Despite this global guidance, there was limited global harmonised approach to the use and purpose of Covid-19 certification documentation. The uses of the certificate varied considerably across the globe. Some governments, including Israel,[48] France,[49] and Italy,[50] amongst others,[51] required the mandatory provision of a certificate to allow access to public life and activities such as public venues such as restaurants, or cultural events. Whilst others never fully developed a policy on their use[52] and with the pandemic having evolved other pending plans have been dropped[53] including for international travel in some instances.[54]

[39] https://www.bbc.com/news/technology-52439145
[40] https://theconversation.com/police-debacle-leaves-the-mcgowan-government-battling-to-rebuild-public-trust-in-the-safewa-app-162850
[41] https://www.dw.com/en/german-police-under-fire-for-misuse-of-covid-contact-tracing-app/a-60393597
[42] https://www.bbc.co.uk/news/world-asia-55541001
[43] https://www.lacapital.com.ar/la-ciudad/controlaran-quienes-incumplieron-elaislamiento-una-app-sus-celulares-n2572740.html
[44] https://web.karisma.org.co/covid-apps-in-colombia-karismas-digital-security-and-privacy-evaluation/
[45] https://fma.ph/2020/07/08/open-letter-to-request-for-strong-user-privacy-protections-in-the-philippines-covid-19-contact-tracing-efforts/
[46] https://www.hhrjournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups/
[47] https://privacyinternational.org/advocacy/4607/covid-19-vaccination-certificates-who-sets-minimum-demands-governments-must-do-even
[48] https://www.theguardian.com/world/2021/feb/28/green-pass-how-are-vaccine-passports-working-in-israel
[49] https://www.theguardian.com/world/2021/jul/12/france-mandates-covid-health-pass-for-restaurants-and-cafes
[50] https://www.loc.gov/item/global-legal-monitor/2021-10-20/italy-government-establishes-stringent-green-covid-19-certification-mandate/
[51] https://www.euronews.com/travel/2021/10/12/green-pass-which-countries-in-europe-do-you-need-one-for
[52] https://www.bbc.co.uk/news/uk-58535258
[53] https://www.aljazeera.com/news/2022/2/17/israel-pm-announces-end-of-vaccine-green-pass
[54] https://www.independent.co.uk/travel/news-and-advice/countries-no-travel-restrictions-tests-unvaccinated-b2071371.html

In particular the mandatory approach to Covid-19 certification raised some serious concerns in terms of discrimination and in particular the impact on already marginalised communities in contexts where access to vaccination was unequal and remained problematic in many parts of the world.[55] These risks and harms were also highlighted by the WHO in its guidance and aligned with its position that such mandatory requirements should not be introduced, at least in the context of international travel, "given that there are still critical unknowns regarding the efficacy of vaccination in reducing transmission."[56]

4.3 Delivery of assistance/social services

The pandemic has also accelerated the digitisation and automation of delivery of social protection programmes by governments and international organisations across the world as governments grappled with the socio-economic crisis which unfolded alongside the health crisis.[57] PI and some of its global partners have documented some of the human rights concerns of these programmes[58] which often result in exclusion of the most vulnerable,[59] arbitrary outcomes and lack of transparency,[60] as well as revealing indiscriminate access to public registration databases by private financial institutions and other intermediaries to facilitate the assessment of eligibility to such programmes.[61]

It is important to note that unfortunately these concerns are not new and were extensively reported by the UN Special Rapporteur on extreme poverty in his report on digital welfare states,[62] and these developments have been observed across the world, including in Colombia, Paraguay, Brazil,[63] the United Kingdom, Uganda, and India to name a few.[64]

[55] https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/abs/veil-of-the-covid19-vaccination-certificates-ignorance-of-poverty-injustice-towards-the-poor/0D8AE039213D7B5F1059FA15D62EEE5A; https://www.the-star.co.ke/news/2021-11-22-amnesty-warns-against-mandatory-vaccination-approach/

[56] https://www.who.int/news-room/articles-detail/interim-position-paper-considerations-regarding-proof-of-covid-19-vaccination-for-international-travellers

[57] See: https://www.unodc.org/unodc/en/press/releases/2020/April/united-nations-secretary-general-launches-plan-to-address-the-potentially-devastating-socio-economic-impacts-of-covid-19.html; https://unsdg.un.org/resources/shared-responsibility-global-solidarity-responding-socio-economic-impacts-covid-19

[58] https://privacyinternational.org/long-read/4582/year-pandemic-welfare-innovation-continues-penalise-poor

[59] See India, https://privacyinternational.org/long-read/4468/failures-digitisation-indias-food-security-programme-exclusion-married-women-odisha

[60] See Colombia, https://privacyinternational.org/long-read/4473/case-solidarity-income-colombia-experimentation-data-social-policy-during-pandemic

[61] See Bolivia, https://www.derechosdigitales.org/wp-content/uploads/identity-systems_ENG.pdf

[62] UN General Assembly, "Report of the Special Rapporteur on extreme poverty and human rights," A/74/493, 11 October 2019

[63] InternetLab, "Brazil's Bolsa Familia Program: the impact on privacy rights", 13 May 2020, published on PI's website and available online at: https://privacyinternational.org/long-read/3758/brazils-bolsa-familia-program-impact-privacy-rights

[64] See: Privacy International's submission on digital technology, social protection and human rights, May 2019, https://privacyinternational.org/advocacy/2996/privacy-internationals-submission-digital-technology-social-protection-and-human; Joints submission to the Special Rapporteurship on Economic, Social, Cultural and Environmental Rights of the Inter-American Commission on Human Rights (IACHR) regarding the situation of Economic, Social, Cultural and Environmental Rights (ESCR) in the region, November 2019, available online at: https://privacyinternational.org/node/3361

5. Digital identity systems rolled out by States and companies

5.1 Role of governments in rolling out digital ID systems

Some of the largest, data-intensive government programmes in the world are national identity systems—centralised government identity schemes that link an individual's identity to a card or number, often using biometric data, and require identity authentication within the system for the provision of public benefits and participation in public life. The discussion surrounding these systems has largely focussed on their perceived benefits empowerment and inclusivity as well as for fraud protection, security, and the delivery of services.[65]

Governments are increasingly rolling out national digital ID systems, making it mandatory for individuals to register in them, justifying its need to do so on a range of aims from facilitating access to public services, to national security and fighting against corruption. These digital identity systems are run by governments, sometimes by private companies, or by a combination of both.

As digital ID systems increasingly require the processing of more data, particularly biometric data, they become more privacy invasive, particularly in the absence of or in a context of weak data protection laws. For example, a comparative study of digital ID systems in countries of the Gulf Council Cooperation (GCC), found that only Bahrain, Qatar, and Saudi Arabia have adopted general laws on data protection. Yet, even these laws contain vague and broad exemptions for data processing by government agencies. The report also found lack of independent oversight over personal data processing in general and over the identification system itself. [66] Various judgments issued by courts around the world, being asked to judge on the implications of identity systems particular on human rights, have taken the position that data protection is a pre-condition and key element of the protection framework which should be in place prior to the deployment if an identity system.[67]

While privacy and data protection issues are central concerns in the implementation of ID systems,[68] as registration in these digital ID systems are demanded to access an increasingly wide range of goods and services, they affect the exercise of a range of human rights. While governments and other proponents of digital ID systems highlight their potential benefits, little attention and public debate has focused on the potential harm that come from the implementation of such systems, notably exclusion, exploitation of personal data, and unlawful surveillance.

[65] Hanmer, L. and Daham, M., 'Identification for Development: Its Potential for Empowering Women and Girls', World Bank, 9 November 2015. Available at: https://blogs.worldbank.org/voices/identification-development-its-potential-empowering women-and-girls; Pokharel, N. and Niroula, S., How a Legal Identity Leads to a Better Life, Open Society Foundations, Voices, 22 January 2015. Available at: https://www.opensocietyfoundations.org/voices/how-legal-identity-leads-better-life)

[66] https://smex.org/the-digital-id-landscape-in-the-gcc-a-mapping-of-programs-regulations-and-human-rights-risks-report-2021/

[67] https://privacyinternational.org/learning-resources/guide-litigating-identity-systems; https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma

[68] https://privacyinternational.org/report/4159/guide-litigating-identity-systems-impact-identity-systems-rights-other-privacy

PI's analysis has shown that the technical characteristics and modalities of the digital ID systems have a significant impact on its compliance with human rights standards.[69] For example, PI has collected many reports of massive data leaks, exclusion from access to benefits and even issues around de-duplication which marred the India's Aadhaar system over the years, showing the significant discrepancy between how the ID systems should work according to its proponents and how they work in practice.[70]

Only when challenged in courts some of the human rights concerns pertaining to digital ID systems such as those described in the following sections are at least partially addressed.[71] This points yet again at the failure of states to provide for adequate legislation and conduct thorough human rights due diligence, including impact assessment, prior to the introduction of digital ID systems.

Exclusion

As recognised by the UN Secretary General in his report on the role of new technologies for the realisation of economic, social and cultural rights: "One major concern linked to comprehensive digital identification systems is that these systems can themselves be sources of exclusion, contrary to their purpose."[72] People are being excluded from accessing some public services as the result of not having a digital ID, because of discriminatory application, technical or logistical barriers or enrolment and verification not being possible. These systems never reach universal coverage, and research in Chile,[73] Uganda,[74] and India[75] has shown, they leave people unable to rights to social security, education and healthcare including some of the most marginalised people as was argued in the case of the ID system in Kenya.[76]

Sometimes the capture of biometric identifiers such as fingerprints is made mandatory to enrol in these systems, despite not everyone having "readable" fingerprints. Exclusion is also likely to happen if someone ends up with an ID that they are not able to make use of e.g. if gender markers assigned on ID is different from their self-identified gender.[77]

[69] https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms
[70] https://privacyinternational.org/case-study/4698/id-systems-analysed-aadhaar
[71] The Mauritian Supreme Court highlighted how security risks associated with biometrics were not adequately defended against, the Aadhaar judgement in India raised concerns around centralised databases, the Supreme Court of the Philippines identified the risk that an individual's movements could be tracked using a national identity system, and the Kenyan High Court specified risks of exclusion as a result of biometric failures as well as other identity system registration failures. https://privacyinternational.org/learning-resources/guide-litigating-identity-systems
[72] https://www.ohchr.org/en/documents/reports/ahrc4329-report-role-new-technologies-realization-economic-social-and-cultural
[73] https://privacyinternational.org/long-read/2544/exclusion-and-identity-life-without-id
[74] https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf
[75] https://privacyinternational.org/long-read/4472/exclusion-design-how-national-id-systems-make-social-protection-inaccessible
[76] https://privacyinternational.org/video/4412/when-id-leaves-you-without-identity-case-double-registration-kenya
[77] https://privacyinternational.org/long-read/4372/my-id-my-identity-impact-id-systems-transgender-people-argentina-france-and

Exploitation

People's data can be exploited through their use and processing within identity schemes. This is particularly the case when 'Unique identifier' is introduced. A 'unique identifier' is a unique number or code, for example an ID number, through which government and the private sector are able to connect together various data sets. The prevalence of this unique identifier across multiple government or private sector databases, implies the risk of providing a "360 degree view" of an individual. On top of this, it raises concerns of further data processing for purposes beyond initial legitimate purpose.

In the ruling of the on Aadhaar in India, the Supreme Court found, "Allowing private entities to use Aadhaar numbers will lead to commercial exploitation of an individual's personal data without his/her consent and could lead to individual profiling."[78]

We have seen this for example also in the context of immigration enforcement and border management. The European Asylum Dactyloscopy Database ("EURODAC") was created for facilitating the application of the Dublin Regulation, which determines the EU Member State responsible for examining an asylum application, but was later made accessible for law enforcement purposes in order to fight terrorism, a purpose for which the data processed was never intended.[79]

In the past, PI has also highlighted concerns about digital identity providing more than the core provision of identity and enabling new services such as age verification which goes beyond the initial status purpose of their system.[80]

Surveillance

ID systems can be used as tools of surveillance within a broader surveillance infrastructure, often leading to disproportionate and unnecessary interference with our privacy and enabling violations of other human rights. In the most concerning cases, the data collected as part of digital ID systems scheme could be used to identify and target perceived opponents, as reported following the Taliban takeover of Afghanistan.[81]

5.2 Role of private companies

While governments bear the primary responsibility for the setting up of digital ID systems, private companies play a significant role in implementing these systems, not only by providing the relevant technologies, but by setting up and managing databases of whole populations. Notably, in December 2016 the French company Civipol was chosen to set-up databases to fingerprint everyone in Mali and

[78] https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf
[79] https://edps.europa.eu/sites/edp/files/publication/09-10-07_access_eurodac_en.pdf
[80] https://privacyinternational.org/long-read/3254/identity-gatekeepers-and-future-digital-identity
[81] https://privacyinternational.org/news-analysis/4615/afghanistan-what-now-after-two-decades-building-data-intensive-systems and https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans

Senegal. Going beyond fingerprinting, it is one of the two companies that are building a full biometric ID-system in Senegal. It also implements a similar project in Côte d' Ivoire. These projects are financed by the EU Trust Fund for Africa.[82]

6. Use of biometrics for identification and authentication

In other sections we have covered some of the uses of biometrics, including in the digital ID systems. Here we focus on the specific concerns raised by the use of biometrics for counter-terrorism purposes.

In its December 2021 analytical briefing on biometrics and counter-terrorism, the United Nations Counter-terrorism Committee Executive Directorate (CTED) notes how "the use of biometrics for counter-terrorism purposes – notably in the context of border management and security – has become increasingly widespread."[83] That is a direct result of UN Security Council resolutions imposing legally binding obligations on all UN member states to develop biometric technologies for counter-terrorism purposes, paired with the strong promotion of these technologies by some, mostly Western states and by powerful industry players. [84]

PI documented in three case studies (covering Afghanistan and Iraq, Israel/Palestine, and Somalia) the human rights implications of the use of biometric technologies for counter-terrorism purposes. While the contexts are different, the main trends are very similar:[85]

- biometric technologies, coupled with large, centralized databases, can seriously undermine the human right to privacy and have an irreversible impact on individuals. In this context, relatively fixed and unchangeable physical features – such as fingerprints – are turned into machine-readable identifiers. Human rights experts are increasingly questioning whether some of these technologies, notably live facial recognition in public spaces, can ever be deployed in ways that do not violate the right to privacy and other human rights, such as freedom of peaceful assembly;

- there is a rising danger of "function creep", notably the gradual widening of a technology use beyond its original, intended purpose;

- biometric technologies can exacerbate exclusion and reproduce racial, ethnic, gender, social class, and other inequalities, as noted by the UN Special Rapporteur on the promotion and

[82] https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric
[83] https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Dec/cted_analytical_brief_biometrics_0.pdf
[84] https://privacyinternational.org/advocacy/4064/briefing-responsible-use-and-sharing-biometric-data-counter-terrorism
[85] https://privacyinternational.org/long-read/4528/biometrics-collection-under-pretext-counter-terrorism

protection of human rights and fundamental freedoms while countering terrorism[86] and the UN Special Rapporteur on contemporary forms of racism;[87]

- many governments rely on the private sector to develop and implement technologies for state surveillance. Industries are well placed to influence government policies and to create the demand for tech solutions. Resulting public private partnerships can introduce vast biometric programs, which are often developed without adequate due diligence and prior human rights impact assessment;[88]

- the rapid deployment of biometrics technologies has not been met by commensurate changes at the level of law or policy in counter-terrorism context. National regulatory and legal frameworks continue to lag behind and, where they do exist, they are rarely effectively enforced, unable to properly safeguard against the hazards and potential misuses of biometrics. The 2021 CTED briefing notes the inadequacy of national legal frameworks, including on data protection and oversight and accountability mechanisms, and states that legislation establishing safeguards "must be developed prior to the implementation of biometric systems".[89]

7. Use of encryption and anonymity technologies

As noted by the UN Human Rights Council, "technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association".[90] In the words of UN High Commissioner for Human Rights "it is neither fanciful nor an exaggeration to say that, without encryption tools, lives may be endangered. In the worst cases, a Government's ability to break into its citizens' phones may lead to the persecution of individuals who are simply exercising their fundamental human rights".[91]

Like we noted in the section above on government hacking, demanding back doors, such as introducing silent listeners, or other exploitation of vulnerabilities pose significant security risks and cannot be targeted to specific users, but would indiscriminately affect any (potentially millions or billions of) users

[86] https://www.ohchr.org/Documents/Issues/Terrorism/SR/Statementtransformative%20technologies_25Juin2021.docx
[87] https://undocs.org/A/75/590
[88] https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships
[89] https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Dec/cted_analytical_brief_biometrics_0.pdf
[90] https://undocs.org/A/HRC/RES/48/4
[91] http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf

of the service.[92] This is because "a backdoor is a technical capability — a vulnerability — that is available to anyone who knows about it and has access to it".[93]

Despite these human rights and security risks, states are often seeking to justify measures to prohibit, limit or undermine encryption, often in the name of preventing and investigating terrorism or child sexual abuse online (such as distribution of child sexual abuse materials or grooming of children.)

For example, in 2016, Russia enacted anti-terrorism legislation requiring communications service providers to indiscriminately retain communications content and data and to be able to provide store, and to submit that data to law-enforcement authorities or security services in cases specified by law together with information necessary to decode electronic messages if they are coded.[94] In November 2018, UK Ian Levy and Crispin Robinson of the UK General Communications Headquarters (GCHQ) published a proposal for "silently adding a law enforcement participant to a group chat or call" ('ghost proposal').[95] On 11 May 2022, the European Commission published a proposal of a draft regulation which, if adopted, would require service providers to monitor of all online communications, both public and private (including on end-to-end encrypted services), for CSAM and grooming content.[96]

Security experts have challenged the claim made by the proponents that these measures do not undermine security and confidentiality of communications.[97]

8. Tracking of internet users

The AdTech (short for "advertisement technology") industry is made up of companies providing tools and services that connect advertisers with target audiences and publishers – such as data brokers, advertisers, apps and platforms.[98] These companies are part of a complex ecosystem where individuals' data is treated as a commodity, collected from websites and digital services on which people rely for vital daily activities – without providing users any control over how their data is shared and repurposed. Companies in the industry then share this data with each other to create finely grained profiles of individuals, which are then used to target people with advertising (commercial and political), and feed

[92] Harold Abelson/Ross Anderson/Steven M. Bellovin/Josh Benaloh/Matt Blaze/Whitfield Diffie/John Gilmore/Matthew Green/Susan Landau/Peter G. Neumann/Ronald L. Rivest/Jeffrey I. Schiller/Bruce Schneier/Michael Specter/Daniel J. Weitzner, 'Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications', Computer Science and Artificial Intelligence Laboratory Technical Report (MIT-CSAIL-TR-2015-026, 6 July 2015).
[93] Bruce Schneier, Evaluating the GCHQ Exceptional Access Proposal (Lawfare, 17 January 2019), https://www.lawfareblog.com/evaluating-gchq-exceptional-access-proposal
[94] This law is being challenged before the European Court on Human Rights. For PI's intervention in one of the cases, see https://privacyinternational.org/legal-action/podchasov-v-russia
[95] Ian Levy/Crispin Robinson, Principles for a More Informed Exceptional Access Debate (Lawfare, 29 November 2018), https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate
[96] Text of the proposal here and related materials: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12726-Fighting-child-sexual-abuse-detection-removal-and-reporting-of-illegal-content-online_en
[97] Bugs in our Pockets: The Risks of Client-Side Scanning, by Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague, Carmela Troncoso, 14 October 2021, https://arxiv.org/abs/2110.07450
[98] https://privacyinternational.org/learn/adtech

into decisions that may negatively affect human rights, such as participation in public affairs, access to health, social security, employment, etc.

Targeted advertising can be discriminatory, manipulative, and exploitative.[99] PI's research has shown that popular websites providing advice and support about mental health share user data with advertisers, data brokers and large tech companies,[100] while some menstruation apps share data with Facebook and other third parties.[101]

Data protection legislation when effectively enforced may offer some protection against abuses such as those described above. Numerous ad tech companies have faced and are still facing investigations by Data Protection Authorities, complaints and lawsuits globally.[102] However, non-compliance with data protection legislation and disregard for the profound impact it can have on individuals' right to privacy and other human rights have led to the ad tech sector being riddled with unlawfully collected data.

9. Discriminatory impacts of privacy invasions on individuals and/or groups at risk

Migrants, asylum seekers and refugees

To respond to migration flows – voluntary or forced – governments worldwide have prioritised an approach to immigration that focuses on security with the aim of controlling, reducing, or preventing entry into their borders and then subjecting to surveillance measures migrants and refugees living on their territory. Increasingly these approaches have been formalised and coordinated as part of a broader strategy to digitise immigration enforcement and border management.[103]

Digital technologies deployed in the context of border enforcement and administration and immigration enforcement reproduce, reinforce, and compound existing human rights violations. Large amounts of data are being requested from migrants, from their fingerprints to the data in their digital devices (see above), while they are often put in a situation of constant surveillance, to assess their credibility and worthiness, and to monitor, track, and profile them. Life-changing decisions are being made based on the data being collected but also inferred and observed, and yet there are limited safeguards in place to regulate and oversee the use of tech and data processing in immigration processes. Decisions, especially

[99] Norwegian Consumer Council, Out of Control – How consumers are exploited by the online advertising industry (14 January 2020), https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf
[100] https://privacyinternational.org/sites/default/files/2019-09/Your%20mental%20health%20for%20sale%20-%20Privacy%20International.pdf
[101] https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data
[102] Footnote: A February 2022joint decision of EU data protection authorities, led by their Belgian counterpart, found that the AdTech industry's trade body "IAB Europe" had committed multiple violations of the EU GDPR in its processing of personal data in the context of its "Transparency and Consent Framework" (TCF) and the Real-Time Bidding (RTB) system. This significant decision has effectively found that the consent mechanism present on 80% of the European internet had "deprived hundreds of millions of Europeans of their fundamental rights" https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-21-2022-english.pdf
[103] https://privacyinternational.org/what-we-do/demand-humane-approach-immigration

when automated, also limit access to effective remedies, particularly in the absence of rationale and accountability.

- In the UK, PI has documented the impact of surveillance driven immigration and border management policies on the rights of migrants and asylum seekers,[104] including collecting testimonies of asylum-seekers who have victims of practices of surveillance and had their benefits cut through the monitoring of their use of the Aspen Card (a kind of debit card given to asylum seekers, on which about £39 is credited every week to cover their basic subsistence needs).[105]

- In Italy, biometric data collected during disembarking operations or at the time of arrival on Italian territory are stored in a database (AFIS) that also contains data on potential criminal suspects. The same database is used to find facial and identity matches by the Italian National Police.[106]

- In Colombia, the proposed regularisation process for Venezuelan migrants included the creation of registry of biometric and demographic data. Concerns raised included insufficient due diligence undertaken prior to assess the implications on those registered and their rights to privacy and non-discrimination, the lack of transparency of data collected, for what purpose, and under what legal basis, in particular in relations to the processing biometric data.[107]

Governments are not the only actors demanding and processing personal data of migrants, asylum seekers and refugees. Humanitarian and development agencies have long processed their personal data from enrolment/registration to identification and authentication. Previously, this data was primary collected directly by these actors, but it is increasingly also being integrated with data from other sources, including from third-parties such as social media data, device-level data, and satellites.[108] The risks of this data being used in ways by governments that put individuals at risk have been exposed, for example in relation to data collected by UNHCR on Rohingyas refugees[109] and in the context of Kenya as noted above.[110]

[104] https://privacyinternational.org/long-read/4790/how-privacy-and-data-protection-law-can-help-defend-migrants-rights
[105] https://privacyinternational.org/campaigns/stop-spying-asylum-seekers
[106] https://www.documentcloud.org/documents/21200979-technologies-for-border-surveillance-and-control-in-italy-identification-facial-recognition-and-european-union-funding?responsive=1&title=1
[107] https://digitalid.karisma.org.co/2021/07/01/sistema-multibiometrico-etpmv/ ; https://digitalid.karisma.org.co/2021/07/01/intervencion-etpmv/ ; https://www.dejusticia.org/lo-que-no-puede-quedar-por-fuera-del-estatuto-temporal-de-proteccion-para-personas-migrantes-venezolanas/ ; https://www.dejusticia.org/column/migracion-y-datos-biometricos-una-peligrosa-mezcla-del-estatuto-de-proteccion/
[108] https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf
[109] https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent
[110] https://privacyinternational.org/video/4412/when-id-leaves-you-without-identity-case-double-registration-kenya

Conclusions

As the above sections sought to illustrate, there are significant challenges in the application of the right to privacy in digital contexts.

Despite repeated recommendations by the UN Human Rights Council and the UN General Assembly[111] to review, amend or enact national laws to ensure respect and protection of the right to privacy, national laws are often inadequate and do not regulate, limit or prohibit surveillance powers of government agencies as well as data exploitative practices of companies.

Even when laws are in place, they are seldom enforced. In fact PI notes how it is often only following legal challenges in national or regional courts that governments are forced to act. This is not a sustainable position: CSOs, journalists, and human rights defenders often do not have the capacity (or legal standing) to challenge governments or companies' actions, they may face threats if they so (including of the same unlawful surveillance that they are challenging) and in many jurisdictions there are no independent avenues of effective redress.

Some surveillance technologies, such as facial recognition and hacking, are unlikely to ever meet the tests of legality, necessity and proportionality under international human rights law. The fact that in the name of countering terrorism and of addressing the dissemination of child sexual abuse materials online, governments seem intentioned to take measures that put the security and confidentiality of all our communications in jeopardy, and as a result threaten the enjoyment of all our human rights.[112]

Companies continue to offer surveillance and data analysis technologies to governments, not only feeding but encouraging a demand for data intensive solutions that usher the introduction of public private partnerships without adequate human rights due diligence and accompanying safeguards. Companies also continue to exploit our personal data, taking advantage of lack of regulation or enforcement.

Finally, we are particularly concerned by the implications of governments failing to adopt a comprehensive human rights-based approach to the use of data and technology is having on other fundamental rights and freedoms, including economic, social, and cultural rights, freedom of expression, freedom of movement, the right to seek refuge.

[111] See examples at https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance
[112] https://privacyinternational.org/learning-resources/privacy-matters