The right to privacy in the digital age
Human Rights Council adopted resolution 48/4
4 June 2022

Submissions of the International Network of Civil Liberties Organizations (INCLO)

INCLO is a network of 15 civil liberties organizations from around the globe.[1] We thank the OHCHR for the opportunity to provide inputs to a report on 'the right to privacy in the digital age (2022)'.[2]

With reference to case studies from INCLO countries, we address recent trends and challenges regarding the right to privacy in relation to (i) measures relying on digital technology taken to combat Covid-19; (ii) facial recognition technologies (FRT); and (iii) use of encryption.

[1] Participating members from INCLO include: the Agora International Human Rights Group (Agora) in Russia, the American Civil Liberties Union (ACLU), the Association for Civil Rights in Israel (ACRI), the Canadian Civil Liberties Association (CCLA), the Centro de Estudios Legales y Sociales (CELS) in Argentina, Dejusticia in Colombia, the Egyptian Initiative for Personal Rights, the Human Rights Law Centre (HRLC) in Australia, the Hungarian Civil Liberties Union (HCLU), KontraS in Indonesia, the Irish Council for Civil Liberties (ICCL), the Kenya Human Rights Commission (KHRC), the Legal Resources Centre (LRC) in South Africa, and Liberty in the United Kingdom.

[2] This submission was drafted by Elizabeth Farries, INCLO Fellow and Co-Director UCD Centre for Digital Policy and Olga Cronin, Programme Manager, INCLO and Policy Officer, ICCL. Research contributions come from Damir Gainutdinov, Kirill Koroteev, Agora; Ben Wizner, Jay Stanley, ACLU; Gil Gan-Mor, ACRI; Brenda McPhail, CCLA; Daniel Ospina, Dejusticia; Ádám Remport, HCLU; Alice Drury, Kieran Pender, HRLC; Martin Mavenjina, KHRC; Auliya Rayyan, Danu Pratama Aulia, Fatia Mauliydianti, KontraS; Edwin Makwati, Sherylle Dass, Devon Turner, LRC; Megan Goulding, Emmanuelle Andrews and Gracie Bradley, Liberty.

We do so with the recognition that international human rights law has provided a 'clear and universal framework for the promotion and protection of the right to privacy'.[3] Privacy is recognised in our digital age as essential for the realization of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association.[4] However, despite these protective frameworks, it is increasingly understood that 'privacy is no longer a social norm'.[5] Technological advancements allow processing of large amounts of personal data, often without the subject's awareness or consent.[6] As more data is collected by governments and companies, 'privacy becomes defined less by the secrets that any piece of information reveals and increasingly by the inferences that large amounts of relatively non-sensitive data make possible—and the power that those inferences grant'.[7] Technologies can have an enormous effect on privacy by amplifying the experiences of the non-digital world, while the benefits are unequally available due to structural inequity.[8]

Protective human rights instruments have been slow to catch up on interrelated privacy and data protection matters. For example, the UN Human Rights Committee General Comment No 16[9] ensures that privacy, under Article 17 of the ICCPR, has taken on enormous new significance since the committee published the comment in 1988.[10] INCLO colleagues previously submitted to the OHCHR input on privacy

---

[3] UN Office of the High Commissioner for Human Rights (OHCHR),International standards, https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx; Under Article 17 of ICCPR, no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, nor to unlawful attacks on their honour and reputation. International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 17; Privacy is also protected by international standards including the Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) art 12, the European Convention for the Protection of Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force 3 September 1953) 213 United Nations Treaty Series 222 (ECHR) art 8, the American Convention on Human Rights (ACHR) (entered into force 18 July 1978) OAS Treaty Series No 36 reprinted in Basic Documents Pertaining to Human Rights in the Inter-American System, OEA/Ser L V/II.82 Doc 6 Rev 1 at 25 (1992) art 11, the Cairo Declaration on Human Rights in Islam (Cairo Declaration) (adopted 5 August 1990, ICFM 1990) Resolution 49/19-P) art 18, Arab Charter on Human Rights (adopted 22 May 2004, entered into force 15 March 2008) reprinted in (2005) 12 International Human Rights Reports 893 arts 16 and 21, the African Commission on Human and People's Rights Declaration of Principles on Freedom of Expression, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Recommendation No. R(99) 5 for the protection of privacy on the Internet, and the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council [2016] OJ L 119 1 (GDPR)

[4] United Nations General Assembly (2014) The Right to Privacy in the Digital Age, A/RES/68/167 United Nations, Human Rights Council Resolution 28/16

[5] Bobbie Johnson, 'Privacy no longer a social norm, says Facebook founder' *Guardian* (London, 11 January 2010) <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> assessed 3 October 2018

[6] B. van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in Serge GutwirthRonald LeenesPaul De Hert (ed), *Data Protection on the Move* (Springer 2016) 411

[7] Ben Green, AFFIDAVIT, *CCLA v Waterfront et al* [2020] Court file no 211/19 (22 May 2019) 11 -12, https://ccla.org/quayside-project-application-documents/

[8] UNHCR, 'Report of the Special Rapporteur on extreme poverty and human rights' (11 October 2019) UN Doc A/74/48037 par. 58

[9] UN Human Rights Committee General Comment No 16, 'Article 17 (Right to Privacy)' (8 April 1988) UN Doc HRI/GEN/1/Rev.9 (Vol. I)

[10] Jamil Dakwar, Elizabeth Farries, Brenda McPhail, Tsanga Mkumba, The right to privacy in the digital age, Human Rights Council adopted resolution 34/7, 2018, INCLO, https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/INCLO.pdf

challenges in the digital age.[11] Here, we reiterate INCLO members' recommendation that the Human Rights Committee issue a new comment on Article 17 as a revision is urgently needed in our digital age.

(i) **Measures relying on digital technology taken to combat the Covid-19 pandemic**

We acknowledge the importance of respecting individuals' right to privacy when designing, developing or deploying technology in response to epidemics and pandemics. We observe that governments in INCLO member countries introduced Covid-19 surveillance technologies which went beyond the purpose of controlling the spread of the disease. INCLO members have analyzed these actions in relation to our set of shared Covid-19 surveillance tech principles that INCLO believes must be adhered to, based on the experience of our members.[12] We detail each of our principles here, and highlight measures INCLO member countries have taken relying on digital technology to combat Covid-19.

Efficacy

Evidence must be established to show that pandemic surveillance tech will be effective prior to deployment, and that efficacy must be routinely reviewed. We saw uptakes of technology in INCLO member countries despite a lack of evidence of efficacy. For example, in the United States, the ACLU describes how temperature checking took place in some workplaces, businesses, and other public venues despite serious questions around the accuracy and efficacy of these tools.[13] Similarly, in Ireland, despite ICCL reaching out multiple times, the government has never offered demonstrable proof for its claim that the Covid Tracker app curbed the transmission of Covid-19.[14]

Primary legislation

Interferences with privacy prompted by Covid-19 surveillance tech by governments should have been backed by primary legislation to allow democratic scrutiny and debate.[15] We have seen an absence of such primary legislation in INCLO member countries. For example, KHRC explains how Kenya lacks a

[11] Ibid

[12] Irish Council for Civil Liberties and others. (2020, May 22). Principles for legislators on the implementation of new technologies' Irish Council for Civil Liberties. https://covid19.inclo.net/inclo-surveillance-tech-and-covid-19-principles/#english

[13] USA: Temperature screening, pandemic drones and workplace contact-tracing apps » COVID-19 Resources Portal (inclo.net), https://covid19.inclo.net/2020/06/24/pic-in-usa-contact-tracing-apps-temperature-screening-immunity-passports/

[14] HSE Covid Tracker App: Pre-Release Report Card, ICCL, 2020, July, https://www.iccl.ie/wp-content/uploads/2020/07/ICCL-DRI-HSE-App-Pre-Release-Report-Card.pdf

[15] Article 17 ICCPR permits interference with the right to privacy only where it is 'authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant, is in pursuit of 'a legitimate aim' and 'meet[s] the tests of necessity and proportionality'. UN General Assembly, 'Promotion and protection of human rights and fundamental freedoms while countering terrorism*Note by the Secretary-General' (23 September 2014) UN Doc A/69/397 par. 30. According to this established standard, interferences with the right to privacy are only permissible under international human rights law if they are neither arbitrary or unlawful. MAPPING, Draft Legal Instrument on Government-led Surveillance and Privacy Including the Explanatory Memorandum, Ver 7.0 (MAPPING Consultation, Feb 2018) par. 11.

comprehensive legislative framework for the use of biometric technologies for surveillance purposes.[16] Similarly, in Russia, Agora describes how 2020 amendments to federal legislation on natural emergencies entered into force, allowing the regions to impose virtually any restriction on human rights in situations of 'high alert'.[17] In Israel, the internal security service, Shin Bet, used counterterrorism surveillance on Covid-19 patients.[18] ACRI submitted a petition to the High Court of Justice opposing this and won.[19]

Necessary and proportionate

Interference with privacy must meet the test of necessity and proportionality.[20] Collecting information, including biometric or health data, must be a necessary and proportionate response.[21] The necessity and proportionality of pandemic surveillance tech is null if the tool's effectiveness cannot be demonstrated and if less intrusive measures would be sufficient to achieve the relevant aim. We have seen unnecessary and disproportionate interferences. For example, in Russia, Agora notes how police in Moscow began monitoring people in quarantine using facial recognition tech cameras warning that a breach of

---

[16] The Kenyan government used CCTV surveillance with intrusive facial recognition technologies during the pandemic to monitor public spaces and enforce social distancing requirementsIt relied on the Computer Misuse and Cyber Crimes Act of 2018 to justify this approach. The Kenyan government also failed to pass laws to regulate where mobile operators could share the geo-location data of self-quarantined individuals. See *Unseen Eyes, Unheard Stories Surveillance, data protection, and freedom of expression in Kenya and Uganda during COVID-19*, April 2021, ARTICLE 19 East Africa, Kenya ICT Action Network, Pollicy, https://www.article19.org/wp-content/uploads/2021/04/EAF-Surveillance-Report_Final-min.pdf; Monyango, F., *Mask or muzzle: The impact of COVID-19 measures on digital rights in Kenya*, African Internet Rights, https://africaninternetrights.org/sites/default/files/Francis%20Monyango.pdf; Maundu C., K*enyan Government's use of surveillance technologies to tackle Covid-19 raises human rights concerns*, 7 October 2021, Global Voices, https://globalvoices.org/2021/10/07/kenyan-governments-use-of-surveillance-technologies-to-tackle-covid-19-raises-human-rights-concerns/

[17] Federal Law of 1 April 2020 no. 98-FZ, amending, in particular, the Federal Law of 21 December 1994 no. 68-FZ "On the Protection of Population from Natural and Industrial Emergencies", http://publication.pravo.gov.ru/Document/View/0001202004010072. More than two years into the pandemic in Russia, is still in a 'high alert' stage.

[18] Israel: Security services cannot collect Covid patients' mobile data without law. https://covid19.inclo.net/2020/07/08/israel-security-services-cannot-collect-covid-patients-mobile-data-without-law/

[19] See We Won: HCJ Sides with ACRI Petition Against Shin Bet Tracking Civilians, ACRI, 26 April 2020, https://www.english.acri.org.il/post/__154 . The High Court ruled that because this practice was deeply invasive of rights it must be brought under the control of primary legislation. See. https://versa.cardozo.yu.edu/opinions/ben-meir-v-prime-minister-0. Subsequently, the Israeli parliament brought in primary legislation justifying this practice, see Kraft, D., *Israel employs controversial tracking tool to fight surging COVID*, Forward, July 8, 2020, https://forward.com/israel/450366/israel-employs-controversial-tracking-tool-to-fight-surging-covid/. ACRI has since filed a petition before the High Court against the General Security Services (GSS) maintaining a database based on sweeping and continuous metadata collection of all citizens and residents, which is open to search and analysis by GSS personnel without a court-ordered warrant. See ACRI, *ACRI Petitions to HCJ: General Security Service Tracking Program - Illegal*, June 1, 2022, https://www.english.acri.org.il/post/__399

[20] Ibid footnote 15, Article 17 ICCPR test .

[21] The European Data Protection Supervisor guidelines for assessing the proportionality of measures that limit fundamental rights to privacy and protection of personal data (2019) EDPS. https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

quarantine rules could lead to a jail term.[22] The tech is inaccurate leading Agora to question whether deployment can be necessary and proportionate.[23]

Independent oversight

Sufficiently resourced and independent oversight mechanisms with technical expertise were required to ensure Covid-19 surveillance tech did not disproportionately interfere with privacy.[24] INCLO members saw a lack of such oversight. For example, in Ireland, when government launched its Covid-19 contact-tracing and symptom-tracking app[25] ICCL called for this oversight mechanism and legislation.[26] While an App Advisory Committee was set up to oversee the app, it barely met[27] and does not include a human rights or privacy/data protection expert. Similarly, in Canada, principles of independent oversight were violated when the Public Health Agency of Canada (PHAC) accessed location data from 33 million mobile devices to monitor people's movements during Covid lockdowns. CCLA saw virtually no public information regarding how precisely the data was used; the parliamentary Standing Committee on Access to Information, Privacy and Ethics subsequently conducted a study and issued a report, calling for a halt to this collection until privacy impacts were fully assessed, and for privacy law reform.[28]

Privacy

We have seen serious privacy concerns in INCLO member countries. For example, in South Africa, the LRC had serious concerns about the government's lockdown regulations that gave the Director General of Health the power to direct an electronic communications service provider to share information on

[22] Russia: Facial recognition cameras used to monitor quarantine compliance in Moscow, » COVID-19 Resources Portal (inclo.net), https://covid19.inclo.net/2020/07/07/russia-digital-passes-frt-cameras-and-mobile-phone-location-data/

[23] Russia's lockdown surveillance measures need regulating, rights groups say. Reuters. April 24, 2020 https://www.reuters.com/article/health-coronavirus-russia-facial-recogni-idINKCN2260CF. Further, covid-positive citizens and their contacts were required to to download a mobile application named 'social monitoring'. Refusal to install would result in a 14-day quarantine at a medical institution. See Moscow Mayor Decree of 5 March 2020 no. 12-UM (https://docs.cntd.ru/document/564377628) and Circular Letter of the Russian Consumer Rights Authority (Rospotrebnadzor) of 11 February 2020 no. 02/2037-2020-32 (https://base.garant.ru/73751146/)

[24] UK Parliament, 'Joint Committee on Human Rights' warning that data protection and privacy standards in relation to a Covid-19 app must be grounded in legislation', 7 May 2020, https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/343/34305.htm#_idTextAnchor012

[25] Ireland: Contact-tracing and symptom-tracking app deployed in response to Covid-19 » COVID-19 Resources Portal (inclo.net), https://covid19.inclo.net/2020/07/07/ireland-contact-tracing-and-symptom-tracking-app-deployed-in-response-to-covid-19/

[26] Elizabeth Farries, Olga Cronin et al, Principles for legislators on the implementation of new technologies, no date, https://www.iccl.ie/wp-content/uploads/2020/06/Principles-for-legislators-on-the-implementation-of-new-technologies.pdf

[27] Cianan Brennan & Daniel McConnell, Covid tracker app committee has met just twice, Irish Examiner, 13 December 2021, https://www.irishexaminer.com/news/arid-40765059.html

[28] Standing Committee on Access to Information, Privacy and Ethics, Report No. 4, "Collection and use of mobility data by the government of Canada and related issues," May 2022. https://www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/report-4/page-5

individuals' location or movement. The High Court of South Africa found this practice unconstitutional[29] and that it unjustifiably infringed privacy rights.[30]

Data protection

Any technological measure that imposes limits on personal data protection necessarily implicates protected privacy rights.[31] Personal data protection must be upheld in all emergency measures; the 'mere existence of a pandemic' is not a sufficient reason to restrict the rights of data subjects.[32] Data protection guarantees for Covid-19 surveillance tech should have included a rights framework, personal data processor obligations, and engagement with a data protection regulator or similar mechanism.[33] However, INCLO members did not see these protections in place. For example, in Israel, the Shin Bet collected in bulk the communications data of all Israelis, and kept it in a database formed to support fighting security threats.[34] In Hungary, the government suspended Articles 15 to 22 of the European GDPR in relation to the processing of personal data,[35] prompting the HCLU and others to write to the

[29] Jennigay Coetzer, Court Deems South Africa's Lockdown Rules 'Irrational' and 'Unconstitutional', ALM LAW.COM, 4 June 2020, https://www.law.com/international-edition/2020/06/04/court-deems-south-africas-lockdown-rules-irrational-and-unconstitutional/?slreturn=20220426162807

[30] South Africa: Handing of mobile phone customers' location data to government is unconstitutional: South Africa: Handing of mobile phone customers' location data to government is unconstitutional » COVID-19 Resources Portal (inclo.net), https://covid19.inclo.net/2020/06/24/pic-in-south-africa-mobile-phone-firms-hand-over-customers-location-data/; and Jennigay Coetzer, Court Deems South Africa's Lockdown Rules 'Irrational' and 'Unconstitutional', ALM LAW.COM, 4 June 2020, https://www.law.com/international-edition/2020/06/04/court-deems-south-africas-lockdown-rules-irrational-and-unconstitutional/?slreturn=20220426162807. Now, new draft Regulations are being proposed which empower environmental health practitioners to engage in search and seizures without warrants where they suspect a health risk. Major concerns regarding privacy and the sweeping powers granted to officials to engage in large-scale data collection under what seems very broad and vague conditions. These are found in the draft National Health Act: Regulations: Surveillance and the control of notifiable medical conditions which can be accessed at https://www.gov.za/sites/default/files/gcis_document/202204/46251gon2051.pdf

[31] The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience, Policy Paper, EDPS, 4 June 2014, https://edps.europa.eu/sites/edp/files/publication/14-06-04_pp_edpsadvisor_en.pdf

[32] Thirtieth Plenary session: EDPB response to NGOs on Hungarian Decrees and statement on Article 23 GDPR, EDPB, 3 June 2020, https://edpb.europa.eu/news/news/2020/thirtieth-plenary-session-edpb-response-ngos-hungarian-decrees-and-statement-article_en

[33] Ada Lovelace Institute, Exit through the App Store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis, April 2020, https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-1.pdf; The European Data Protection Supervisor guidelines for assessing the proportionality of measures that limit fundamental rights to privacy and protection of personal data, EDPS, 2019, https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[34] During Covid, the Ministry of Health gave the Shin Bet the names of all Covid-19 patients. The Shin Bet searched its database to find their locations and contacts and gave the Ministry of Health the list of those contacts. The Ministry of Health sent them a text message to start quarantine and they were put on police lists for quarantine enforcement. See Rights & COVID-19: Privacy, The Association for Civil Rights in Israel, 25 April 2020, https://www.english.acri.org.il/post/__188-1

[35] Hungary: Man arrested for Facebook post as data protection rights suspended in response to Covid » COVID-19 Resources Portal (inclo.net),

European Data Protection Board.[36] Further, in Colombia, CoronApp was transferred to the Ministry of Health, which meant changing its name and possible uses, and transferring its data to another public entity without notifying its 11 million users.[37] This modification was done without any consideration for the principles of necessary and proportionate data use.

Protest

Privacy is protective of protest rights, and governments and policing institutions have positive obligations to protect the right to protest.[38] A pandemic must not be a reason to target those who encourage participation in or attend protests, with surveillance tech or otherwise. However, we saw this in some INCLO member countries. For example, in Indonesia, there was social media monitoring and the arrest of hundreds of political protesters[39] as the government vowed to crack down on Covid-19 disinformation. KontraS believes the phone hacking and arrest of one individual were in relation to his criticisms of the government online.[40]

Expression

Privacy is similarly protective of the right to freedom of expression and to hold opinions[41] and does not impede the fight against Covid-19. Pandemic surveillance tech must not be used to target those who speak out or who are critical of those in power. However, we saw limitations on free expression in INCLO member countries. For example, in Argentina, social media monitoring by police and security forces became more widespread during Covid. A man was arrested for a sarcastic tweet in which he joked: 'Che, what's up, for those of us who don't collect the 10,000 peso bonus, the looting still stands, right?'.[42]

---

https://covid19.inclo.net/2020/07/07/pic-in-hungary-suspends-data-protection-rights-man-arrested-for-facebook-post/. The government reinstated the suspended Articles when it ended the special legal regime on 18 June 2020.

[36] Ibid

[37] Disponible la aplicación de MinSalud para descargar el certificado de vacunas, La Republica, 30 November 2021 https://www.larepublica.co/economia/ya-esta-disponible-la-aplicacion-de-minsalud-para-descargar-el-certificado-de-vacunas-3268904

[38] Privacy in our digital age is essential - in and of itself - but also for the realization of other recognised rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association. Resolution 28/16, 'The Right to Privacy in the Digital Age' (21 January 2014) UN Doc A/RES/68/167

[39] Tri Indah Oktavianti and Budi Sutrisno, *New 'virtual police' adds to fears over loss of online civic space, civil freedoms*, The Jakarta Post, 19 March, 2021, https://www.thejakartapost.com/news/2021/03/19/new-virtual-police-adds-to-fears-over-loss-of-online-civic-space-civil-freedoms.html

[40] Police circular called 'Awareness of Ethical Culture to Create Clean, Healthy and Productive Indonesian Digital Space'. Ravio Patra, a vocal critic of the Indonesian government and its response to Covid-19, was arrested hours after his phone was hacked resulting in a message going out calling people to riot.
Indonesia: Critic of Covid-19 response arrested after phone hack and WhatsApp call to riot » COVID-19 Resources Portal (inclo.net)
https://covid19.inclo.net/2020/07/07/pic-in-indonesia-political-critic-is-arrested-and-detained-after-phone-hack/

[41] Privacy in our digital age is essential - in and of itself - but also for the realization of other recognised rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association. Resolution 28/16, 'The Right to Privacy in the Digital Age' (21 January 2014) UN Doc A/RES/68/167

[42] @KevinGuerra99, Twitter, 8 April 2020, https://twitter.com/KevinGuerra99/status/1247709948554903554?. Two days later he was informed that he was under criminal investigation. Argentina: Man arrested for sarcastic tweet amid social media intelligence during Covid-19 » COVID-19 Resources Portal (inclo.net), https://covid19.inclo.net/2020/07/07/pic-in-argentina-social-media-intelligence-man-arrested-after-tweet/. The Argentine government has subsequently issued two Resoluciones (Resolución 31/2018 Secretaría de Seguridad de

CELS defended Mr Guerra, arguing these forms of open source intelligence infringe the right to freedom of expression. He was later found innocent with the judge stating his posts did not constitute a crime.[43]

Purpose limitation

Clear purpose limitation is important to ensure that the original intentions for Covid-19 surveillance tech don't gradually shift into more pervasive forms of surveillance that extend beyond Covid-19.[44] We are seeing trends where purpose limitation is not being deployed. For example, in Colombia, a national app which started out as a tool for informational purposes[45] and health self-evaluation morphed[46] into an app with location tracking and proximity contagion tracking features and eventually a 'mobility passport'.[47] Despite criticisms from Dejusticia and others, the government first removed the contact-tracing element from the app and then reincorporated it to its multi-purpose app.[48] maintains a database based on sweeping and continuous metadata collection of all citizens and residents, which is open to search and analysis by GSS personnel without a court ordered warrant. In Israel ACRI has

Consent

It is the position of INCLO members that the use of any Covid-19 surveillance tech must be entirely voluntary and not mandatory – in law or effect. People's access to rights guaranteed by law must not be conditional on the use of these technologies. However, in Hungary, the mass collection of email addresses by the Hungarian government in the course of vaccine registration at the website vakcinainfo.gov.hu occurred without genuine consent, and was subsequently used for political direct

---

la Nación; Resolución 144/2020 - Ministerio de Seguridad, https://www.boletinoficial.gob.ar/detalleAviso/primera/230060/20200602) in support of these open source intelligence activities undertaken by police officers. The stated purpose is crime prevention. There is no clear criteria for this.

[43] Juzgado Federal de Mar del Plata Nº 3, causa Nº 8256/2020, caratulada 'IMPUTADO: GUERRA, KEVIN s/INTIMIDACION PUBLICA, resolución del 10 de noviembre de 2020.

[44] Ada Lovelace Institute "Exit through the App Store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis" https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-1.pdf

[45] Laura Gamba, Colombian president launches app to track COVID-19, AA, 9 March, 2020, https://www.aa.com.tr/en/americas/colombian-president-launches-app-to-track-covid-19/1759011

[46] Carolina Botero, Pilar Sáenz, Stéphane Labarthe, Andrés Velásquez, ¿Qué dice que hace y qué es lo que realmente hace CoronApp? Fundación Karisma, 23 April 2020. https://web.karisma.org.co/que-dice-que-hace-y-que-es-lo-que-realmente-hace-coronapp/

[47] Jorge Cantillo, Cómo funciona la aplicación del Gobierno colombiano para salir a la calle, infobae, 15 April 2020, https://www.infobae.com/america/colombia/2020/04/15/como-funciona-la-aplicacion-del-gobierno-colombiano-que-sera-obligatoria-para-salir-a-la-calle/

[48] Colombia: Covid-19 information app morphs into location-tracking tool » COVID-19 Resources Portal (inclo.net), https://covid19.inclo.net/2020/06/24/pic-colombia-contact-tracing-app-drones-and-thermal-cameras/. Note that the CoronApp source code was not made publicly available, despite being based on an open GNU GPL v3 license — that requires transparency of the source code once the application is released to the public. The Colombian Constitutional Court is about to decide if the source code should be made publicly available, thanks to a judicial action filed by Dejusticia. https://www.dejusticia.org/litigation/intervinimos-en-dos-casos-ante-la-corte-constitucional-relacionados-con-la-aplicacion-coronapp/

marketing[49], especially before the general elections. Similarly, in Ireland, one year after the app was launched, a feature was added to the app which allowed people to 'register' their EU Covid-19 Certificate, a European-wide proof of vaccination. This coincided with the passing of a new domestic law which required people to show proof of Covid-19 vaccination or recovery to access indoor hospitality. People who could not, or did not wish to, show this proof could not eat or drink indoors for 7 months. In Colombia, using the Government-created app was mandatory to pursue certain activities, including air travel. Journalists criticized this measure given its potential risk to source confidentiality.[50] The Constitutional Court recently reminded the national government to respect the citizens' right to consent even in health emergency crises.[51]

Transparency

Pandemic surveillance tech deployment must be wholly transparent in order to ensure accountability.[52] It must disclose what data is acquired, how it will be used, who it will be shared with, how long it will be retained, and when and how the data systems will be destroyed. However, we have seen a lack of transparency, and accountability in INCLO member countries. For example, in Australia, the HCLU appealed for the government to publish the specific design, operation, intention and privacy and data protection safeguards of the then pending contact-tracing app,[53] but they were not published until after the app's launch. Within hours of its launch, experts highlighted[54] serious privacy issues with the app.[55]

Non Discriminatory

Pandemic surveillance tech, whether by intention or effect, must not be used to target, harass or punish vulnerable populations. However, the deployment of tech has led to discriminatory impacts of privacy invasions on individuals and/or groups at risk. For example, the CCLA advocated against the use of data-driven initiatives which serve to discriminate, stigmatize, or deny fundamental rights.[56] This includes privacy-invasive Artificial Intelligence-based risk assessment apps which exacerbate concerns regarding

---

[49] Dr. Zsuzsa Sándor, Így lett az oltásinformációból ellenzéki lejáratás, 24.hu, 2 April 2022, https://24.hu/belfold/2022/04/02/vakcinainfo-kormanyzati-tajekoztatas-alkotmanybirosag-kuria-sandor-zsuzsa-velemeny/

[50] Fundación para la Libertad de Prensa FLIP, "CoronApp pone en riesgo a las y los periodistas", 16 de septiembre de 2021, https://www.facebook.com/watch/?v=888307365137837

[51] Corte Constitucional, comunicado de prensa, sentencia T-143 de 2022, https://www.corteconstitucional.gov.co/noticia.php?En-estudio-de-tutela-contra-CoronApp,-Corte-advierte-que-Gobierno-est%C3%A1-obligado-a-aplicar-legislaci%C3%B3n-y-jurisprudencia-constitucional-en-materia-de-habeas-data-para-tratamiento-de-datos-personales-9275

[52] See for example how The European Digital Services Act package represents new legislative frameworks to address transparency with accountability. Read more at Niamh Kirk, Elizabeth Farries, Kalpana Shankar, Eugenia Siapera. The Digital Services Act Package: A Primer, UCD Centre for Digital policy, no date, https://digitalpolicy.ie/the-digital-services-act-package-a-primer/

[53] Daniel Webb, HRLC letter to Hon Greg Hunt MP Minister for Health, 3 April 2020, https://static1.squarespace.com/static/580025f66b8f5b2dabbe4291/t/5e8d1e5f80029314491f5e52/1586306663679/Covid+app+letter+to+health+dept+%281%29.pdf

[54] Australia: Covid-19 app lacks transparency as siren-equipped drones monitor social distancing, COVID-19 Resources Portal (inclo.net), https://covid19.inclo.net/2020/07/07/pic-in-australia-contact-tracing-app-drone-use/

[55] vteague / contactTracing https://github.com/vteague/contactTracing/blob/master/blog/2020-04-27TracingTheChallenges.md

[56] Brenda McPhail, Data Surveillance by Canadian Governments as COVID Response: CCLA's Privacy Protection Prescription, CCLA, 20 April 2020, https://ccla.org/coronavirus-update-data-surveillance/

differential impacts for vulnerable populations.[57] The contact tracing via the CovidAlert app had potentially discriminatory effects in that a reasonably expensive smartphone capable of running a recent operating system was required. People at the intersection of race, poverty, gender and relative newness to Canada were most at risk and least likely to have access to the app meant to mitigate their risk. Similarly, as Australia transitioned away from the use of hotel quarantine to manage its international arrivals, a mandatory app was proposed to ensure compliance with the required 14-day home quarantine requirements. The facial recognition element did not satisfy the non-discriminatory principle in INCLO's framework, due to the racial and gender biases inherent in the app.[58]

Safeguarded from commercial interests

Our personal data must be protected from analytical tracking technologies seeking to collect our movements, behaviors and health status for profit. Any sharing of health data with third-party companies must be strictly safeguarded against. In the UK, Liberty was seriously concerned about the involvement of private companies such as Palantir and British artificial intelligence start-up Faculty in the British government's NHS Test and Trace system.[59] This partnership would have seen the transfer of health data concerning millions of UK citizens to private tech companies.[60] However, the partnership was later abandoned by the government, following litigation from openDemocracy and Foxglove.[61]

Non-punitive

Covid-19 surveillance tech must not be used for any punitive purpose or legal proceedings. However, in Kenya, electronic and mobile phone surveillance was used to round up people who had escaped from quarantine centers or to enforce the mandatory 14-days of quarantine rule.[62] Some people reported that they were not allowed out of the detention facilities until they paid their nightly fees for the detention despite claims by the government that they would cover the costs.[63] The KHRC was concerned about unlawful arrests and detention in the pretext of enforcing curfew and extortion and bribery by police. Further, in a New Dehli court, people accused of crimes were ordered to download the mandatory

---

[57] Canada: Watchdog warns against Covid-19 tech tools which discriminate, stigmatise, or deny rights » COVID-19 Resources Portal (inclo.net), https://covid19.inclo.net/2020/07/07/pic-in-canada-contact-tracing-apps-thermal-cameras-machine-learning/

[58] Josh Taylor, Home quarantine apps spark privacy fears over facial recognition and geolocation technology, The Guardian, 13 October, 2021, https://www.theguardian.com/australia-news/2021/oct/13/home-quarantine-apps-prompt-privacy-and-racial-bias-concerns-in-australia

[59] Natasha Lomas, UK's COVID-19 health data contracts with Google and Palantir finally emerge, Tech Crunch, 5 June 2020, https://techcrunch.com/2020/06/05/uks-covid-19-health-data-contracts-with-google-and-palantir-finally-emerge/?

[60] UK: Centralised app abandoned as private firms embedded in government's collection of health data » COVID-19 Resources Portal (inclo.net) https://covid19.inclo.net/2020/07/07/liberty-private-firms-involved-in-uk-government-collection-of-health-data/

[61] Cori Crider, The UK government has ended Palantir's NHS data deal. But the fight isn't over, openDemocracy, 15 September 2021 https://www.opendemocracy.net/en/ournhs/the-uk-government-has-ended-palantirs-nhs-data-deal-but-the-fight-isnt-over/

[62] Cyrus Ombati, State taps phones of isolated cases, The Standard, 24 March 2020, https://www.standardmedia.co.ke/article/2001365401/state-taps-phones-of-isolated-cases

[63] Kenya: Surveillance tech used to enforce mandatory $65-a-night quarantine, » COVID-19 Resources Portal (inclo.net), https://covid19.inclo.net/2020/07/07/pic-in-kenya-aerial-surveillance-app-mandatory-costly-quarantine/

contact-tracing app and register as a 'Covid-19 warrior' as part of their bail conditions, a practice that occurred in courts across India.[64] Employees also faced criminal penalties if they didn't download contact-tracing apps.[65]

In conclusion, we have seen in INCLO countries how governments did not adhere to best practices, as expressed in our Covid-19 surveillance tech principles. In INCLO countries, state authorities relied on digital technologies to combat the Covid-19 pandemic that did not protect and respect the right of individuals to privacy and related rights in their design, development or deployment.

(ii) Facial recognition technologies (FRT)

INCLO members documented in its 2021 report on FRT, which details 13 FRT case studies from around the world,[66] a number of trends and challenges with regard to the human right to privacy, including those addressed in the present resolution. FRT has the potential to render our internationally-recognised right to privacy illusory. While its lack of accuracy exhibits bias against anyone who is not a white male, leading to concerns in a policing context of undue and discriminatory detention and arrrest, we don't want the tech to improve because accurate FRT can make it impossible for anyone to move through public spaces and remain 'just a face in the crowd'.[67] We detail our concerns here and conclude with a call advocating a full moratorium against policing FRT.

Lack of accuracy leading to racial and gender biases

These systems are infamously inaccurate.[68] Nonetheless, INCLO members are witnessing deployment of policing FRT. Policing FRT is simply not advanced enough for policing purposes.[69] Of particular concern are the racial and gender biases in the tech. They are more likely to misidentify black and brown people

[64] Apoorva Mandhani, Courts set new bail conditions — register as 'Covid-19 warrior', download Aarogya Setu app, The Print, 20 May 2020, https://theprint.in/judiciary/courts-set-new-bail-conditions-register-as-covid-19-warrior-download-aarogya-setu-app/425589/

[65] India: Employees face criminal penalty if they don't download contact-tracing app » COVID-19 Resources Portal (inclo.net), https://covid19.inclo.net/2020/07/07/pic-in-india-mandatory-contact-tracing-app-ai-equipped-police-drones/

[66] In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World, January 2021, INCLO, https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf

[67] Brenda McPhail maps the experience of INCLO member countries with FRT and the right to privacy at p17 in See In Focus Facial Recognition Technologies and Rights Harms from Around the World January 2021 INCLO, https://files.inclo.net/content/pdf/19/in-focus-facial-recognition-tech-stories.pdf

[68] Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification Joy Buolamwini and Timnit Gebru, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

[69] Brian Hutton, Facial recognition technology 'not advanced enough' for use by Garda, Irish Times, 25 May 2022, https://www.irishtimes.com/crime-law/2022/05/25/facial-recognition-technology-not-advanced-enough-for-use-by-garda/

over white people and also women over men.[70] Police must not deploy inaccurate tech which leads to wrongful detentions or arrests of people who are already marginalized due to their race and/or gender.[71]

Discrimination due to overpolicing

That policing FRT misidentifies people who are not white men is a form of discrimination in itself. However, even if the tech were accurate, it would result in a power asymmetry between residents and police, and likely exacerbate problems with over policing in neighborhoods with minority groups.[72] Over policing leads to disproportionate incrimination in these communities.[73] For example, it has emerged the Israeli military uses FRT to surveil Palestinians en masse, despite refusing to acknowledge this when being asked under Freedom of Information laws.[74] The surveillance involves smartphone technology called Blue Wolf which captures photographs of Palestinan faces, runs them through a database and then the app flashes either yellow, red or green to indicate whether a person should be detained, arrested or allowed to pass. The database was created by Israeli soldiers taking part in a competition to photograph Palestinians, with prizes for the most pictures collected by each unit.

Undue surveillance

The capacity of FRT to scan everyone's face in the crowd is very dystopic in character.[75] FRT is different from cameras. It doesn't just see you, it has the capability to connect to databases holding detailed information on you. The tech is objectifying - reducing people to objects to be scanned.[76] INCLO

---

[70] UK's Metropolitan Police FRT found to have an error rate of 81 per cent, see 81% of 'suspects' flagged by Met's police facial recognition technology innocent, independent report says, Sky News, July 2019, https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941; MIT and Stanford University tested three different commercial FRT systems; less than 1% eros for light skinned men, 20% of the cases related to faces of dark-skinned women, see Study finds gender and skin-type bias in commercial artificial-intelligence systems, MIT News, February 2018, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212; US National Institute of Standards and Technology says FRT suffers from a significant bias that leads to misidentifications of people of African and Asian descent, see Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NIST, December 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

[71] Robert Williams was incorrectly identified by policing FRT leading to him being handcuffed and arrested at his home in front of his wife and two daughters before being detained for 30 hours, see ACLU, Wrongfully Arrested Because of Flawed Face Recognition Technology, Youtube, June 2020, https://www.youtube.com/watch?v=Tfgi9A9PfLU&feature=youtu.be

[72] Morgan Klaus Scheuerman, Madeleine Pape, Alex Hanna. (2021) Auto-essentialization: Gender in automated facial analysis as extended colonial project. Big Data & Society 8:2. See also Dwoskin E, Israel escalates surveillance of Palestinians with facial recognition program in West Bank, Washington Post, 8 November 2021, https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html; Jeffrey Dastin, Amazon extends moratorium on police use of facial recognition software, 18 May 2021, Reuters, https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/

[73] See In Focus Facial Recognition Technologies and Rights Harms from Around the World January 2021 INCLO, https://files.inclo.net/content/pdf/19/in-focus-facial-recognition-tech-stories.pdf, p9

[74] See Twitter thread from Director of the Civil and Social Rights units, ACRI Gil Gan-Mor, https://twitter.com/Gil_GanMor/status/1457623046655709192

[75] Liberty wins ground-breaking victory against facial recognition tech, Liberty, August 2020, https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/

[76] Human dignity requires that individuals are not treated as mere objects. FRT calculates existential and highly personal characteristics, the facial features, into a machine-readable form with the purpose of using it as a human

members do not want FRT to move society towards a scenario where police build databases of innocent people unchecked in order to make raw powerful analytic inferences about them.[77] This technology has the potential to deny presumptions of innocence in an always-on surveillant network, fundamentally changing the relationship between citizen and state. For example, in Israel, the government has approved a draft bill that would allow the police to use FRT with very minimal limitations.[78]

Necessity and proportionality

Surveillance powers of policing FRT intrude on the rights to privacy, and its associated rights including protection of personal data, freedom of expression, peaceful assembly and association.[79] Laws providing for the introduction and expansion of state surveillance powers must meet the test of necessity and proportionality or else risk arbitrary and unlawful infringement of these rights.[80] While public safety and national security can sometimes override our rights, the significant risks listed here presented by policing FRT challenge the tests of necessity and proportionality.[81]

Mass and targeted surveillance

FRT and other biometric surveillance tools enable mass surveillance and discriminatory targeted surveillance.[82] They can identify and track people everywhere they go. This is not restricted to the level of the individual. FRT capabilities can be very powerful. In searching for an individual, the tech can scan at the level of community - locating and analyzing individuals with whom a suspect is associated.[83]

Purpose limitation

---

license plate or ID card, thereby objectifying the face. See Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Version 1.0, adopted on 12 May 2022, European Data Protection Board, edpb-guidelines_202205_frtlawenforcement_en_1.pdf par. 40.

[77] Jay Stanley, A Scary Demonstration of What Unchecked Face Recognition Could Look Like, ACLU, 8 February 2022, https://www.aclu.org/news/privacy-technology/a-scary-demonstration-of-what-unchecked-face-recognition-could-look-like

[78] "Surveillance Law" Memorandum: Genuine Risk to Democracy and Human Rights, ACRI, August 2, 2021, https://www.english.acri.org.il/post/__344

[79] Privacy in our digital age is essential - in and of itself - but also for the realization of other recognised rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association. Resolution 28/16, 'The Right to Privacy in the Digital Age' (21 January 2014) UN Doc A/RES/68/167

[80] For example, Article 17 ICCPR permits interference with the right to privacy only where it is 'authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant, is in pursuit of 'a legitimate aim' and 'meet[s] the tests of necessity and proportionality'. UN General Assembly, 'Promotion and protection of human rights and fundamental freedoms while countering terrorism*Note by the Secretary-General' (23 September 2014) UN Doc A/69/397 par. 30

[81] See In Focus Facial Recognition Technologies and Rights Harms from Around the World January 2021 INCLO, https://files.inclo.net/content/pdf/19/in-focus-facial-recognition-tech-stories.pdf

[82] See for e.g. Elizabeth Carthy, ICCL Submission on the General Scheme of the Garda Síochána (Powers) Bill, August 2021, https://www.iccl.ie/wp-content/uploads/2021/12/210813-FINAL-ICCL-Submission-Police-Powers-Bill.pdf par. 40

[83] Jay Stanley, A Scary Demonstration of What Unchecked Face Recognition Could Look Like, ACLU, 8 February 2022, https://www.aclu.org/news/privacy-technology/a-scary-demonstration-of-what-unchecked-face-recognition-could-look-like

There is a real risk that this tech, once deployed for policing purposes, will not be contained according to strictly limited purposes.[84] A broad range of purposes also go against the requirement that any infringement on rights must be as minimal as possible to achieve a specified legitimate aim. Will permitting policing FRT surveillance tech mark a point of no return?[85] How well can legislation contain the normalized impact of this tech and the scope creep that it potentiates?

Data protection

We have serious concerns about policing FRT that is not compatible with data protection principles associated with privacy rights.[86] We have also witnessed authorities' lax compliance with data protection laws through their use of CCTV, ANPR, drones and body worn cameras.[87] It is important for authorities to demonstrate in the first instance a real commitment to, and understanding of, data protection law, before expanding surveillance with the use of tech that can capture people's sensitive biometric data.

Commercial and industry interests

The involvement of commercial interests in policing FRT raise concerns for policing practice. Clearview AI, a facial recognition company used by British police (and police in many other countries[88]), has been fined more than £7.5m for creating an unlawful database of 20 billion images.[89] Given policing

---

[84] See for example the purpose limitation define in Article 5(1)(b) of the GDPR

[85] India used FRT and driving licence and voter identity databases to 'identify' 1,900 protesters during assemblies in Delhi in February 2020 Delhi violence: Over 1900 faces recognised through facial recognition, says Amit Shah, The Economic Times, March 2020, https://economictimes.indiatimes.com/news/politics-and-nation/delhi-violence-over-1900-faces-recognised-through-facial-recognition-says-amit-shah/articleshow/74605677.cms?from=mdr; In Argentina, A woman identified by an FRT camera in Buenos Aires was intercepted by police officers and detained in 2019, several years after the expiration of an arrest warrant that had been issued against her. The order had originally been issued in 2006 for the woman's failure to testify in court as a witness because she had not been duly notified of her obligation. By the time she was detained in 2019, the warrant she knew nothing about had long expired, making her arrest illegal. See In Focus Facial Recognition Technologies and Rights Harms from Around the World January 2021 INCLO, https://files.inclo.net/content/pdf/19/in-focus-facial-recognition-tech-stories.pdf p20

[86] The European Data Protection Supervisor guidelines for assessing the proportionality of measures that limit fundamental rights to privacy and protection of personal data (2019) EDPS. https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

[87] See for e.g. Elizabeth Carthy, ICCL Submission on the General Scheme of the Garda Síochána (Powers) Bill, August 2021, https://www.iccl.ie/wp-content/uploads/2021/12/210813-FINAL-ICCL-Submission-Police-Powers-Bill.pdf par. 40; DPC Ireland 2018 - 2020 Regulatory Activity Under GDPR, Data Protection Commission, June 2020, https://www.dataprotection.ie/sites/default/files/uploads/2020-06/DPC%20Ireland%202018-2020%20Regulatory%20Activity%20Under.pdf, p63

[88] For example, in Canada the Privacy Commissioner of Canada conducted two investigations into the use of Clearview AI tools by policing bodies in Canada and issued scathing findings. See "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta," https://priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/ and "Police of of facial recognition technology in Canada and the way forward," https://priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/. See also Mac, R., *Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here*, Buzzfeed, August 25, 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table

[89] Facial recognition company used by British police fined £7.5m, 24 May 2022, Independent, https://www.independent.co.uk/topic/facial-recognition

authorities tend to be shielded from information requests of the public,[90] people may not know which companies police are using. However, we do know that companies in the past have agreed to sell this tech to policing forces. Given public pressure over risks, some companies have paused selling technology to police.[91]

In conclusion, the risks presented by FRT are significant enough to prompt several international organizations to call for the implementation of safeguards in national legislation.[92] However, it is the belief of INCLO members in this submission that FRT used to facilitate mass surveillance in a policing context **cannot be adequately** safeguarded by legislation. There are currently **no circumstances** in which such policing FRT can safely be rolled out. We have seen similar calls made by academics, civil societies,

[90] Elizabeth Farries and Eric King, Unanswered Questions: International Intelligence Sharing, (2018) INCLO, https://files.inclo.net/content/pdf/23/unanswered_questions.pdf

[91] Amazon and Microsoft paused selling they will not sell FRT to police in the US, see Despite pausing sales to police, company has not made same commitment for sales to federal law enforcement, ACLU, June 2020; and in March 2020, Microsoft pulled its financial support for AnyVision - a company that sold FRT to Israel for deployment at West Bank/OPT checkpoints to verify Palestinians' identities as they enter Israel, see The Global State of Facial Recognition, Digital Information World, July 2020, https://www.digitalinformationworld.com/2020/07/the-global-state-of-facial-recognition-infographic.html and Face Recognition Lets Palestinians Cross Israeli Checkposts Fast, But Raises Concerns, NPR, August 2019 https://www.npr.org/2019/08/22/752765606/face-recognition-lets-palestinians-cross-israeli-checkposts-fast-but-raises-conc?t=1606406049254; In Canada, Clearview AI, which scrapes images from social media sites, builds a database, and offers clients, including law enforcement agencies, access to that database, withdrew from the country. This followed the launch of a probe into the use of the tech by police by the Privacy Commissioner. See The Secretive Company That Might End Privacy as We Know It, New York Times, Kashmir Hill, January 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html and Clearview AI ceases offering its facial recognition technology in Canada, Office of the Privacy Commissioner of Canada, July 2020, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/. See also ACLU, In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law, May 9, 2022, https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois

[92] Urgent action needed over artificial intelligence risks to human rights, https://news.un.org/en/story/2021/09/1099972, United Nations News, 15 September, 2021; Facial recognition technology: fundamental rights considerations in the context of law enforcement, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, p.33, European Union Agency For Fundamental Rights, 2019; Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, European Data Protection Board, May 2022, https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

politicians and stakeholders around the world.[93] It is important for policing authorities and governments to recognize the dangers of this intrusive tech such that a full moratorium against its use is installed.

(iii) Use of encryption

While recognising that encryption plays an important role in protecting privacy and related rights, and against states' trends of mandating backdoors without evidence this increases national security, nine INCLO members submitted a third-party intervention to European Court of Human Rights on Russia's ban of Telegram over the app's refusal to hand over encryption keys.[94]

Encryption plays an important role in protecting privacy

Encryption is important to ensure the enjoyment of the rights to privacy and expression.[95] The privacy afforded by encryption provides advantages to populations who are discriminated against or face 'reprisals or unwanted attention' by providing them with safe forums to congregate, organize, mobilize, build communities.[96] This includes, among others, women, investigative journalists, lawyers, human rights defenders, activists, and civil society organizations. It allows people to seek, receive, and impart

---

[93] In Moscow, protesters lodged a complaint with the European Court of Human Rights, over Russia's use of FRT at protests, see Milov filed a lawsuit against the Moscow authorities and the Central Internal Affairs Directorate over face recognition technology, Kommersant, January 2020, https://www.kommersant.ru/doc/4227471; in Israel, refusals by the Israel Police and Israel Defence Forces to reveal the use of FRT in both Israel and West Bank/Occupied Palestinian Territories has been met with resistance from ACRI, see Police and Military Use of Facial Recognition Technology, ACRI, September 2020, https://www.english.acri.org.il/post/__244; 200 civil society organiation, academics, technologist, experts and activists have signed petitions seeking a full ban, see 07 June 2021 Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance, https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf; The European Parliament called for a ban on facial recognition through a non-binding resolution and also asked for an AI-based predictive policing ban - see European Parliament calls for a ban on facial recognition, Non-binding resolution also asks for AI-based predictive policing ban 6 October 2021, PoliticoPro, https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/; Multiple cities have put in an outright ban against police using FRT in locations, such as San Francisco, Berkeley and Oakland in California, as well as Cambridge, Springfield, and Somerville in Massachusetts. See In Focus Facial Recognition Technologies and Rights Harms from Around the World, January 2021, INCLO, https://files.inclo.net/content/pdf/19/in-focus-facial-recognition-tech-stories.pdf at p10.

[94] Submitted by ICCL, CCLA, CELS, Dejusticia, HCLU, KHRC, KontraS, LRC, Liberty. Application no. 13232/18 TELEGRAM MESSENGER LLP and TELEGRAM MESSENGER INC. against Russia, 21 January 2021, https://files.inclo.net/content/pdf/71/Telegram_v_Russia_-_ICCL___Others_TPI_-_Written_Submissions__FINAL_-combined__3_.pdf

[95] The right to privacy in the digital age: resolution adopted by UN General Assembly (75th session 2020-2021) A/RES/75/176, par.9; See Office of the High Commissioner for Human Rights, The Right to Privacy in the Digital Age, 30 June 2014 (A/HRC/27/37); UN General Assembly Resolution 68/167, 18 December 2013 (available at A/RES/68/167); Report of the Special Rapporteur, 10 August 2011 (A/66/290); and Report of the Special Rapporteur, 17 April 2013 (A/HRC/23/40)

[96] Noman, Helmi, Arab Religious Skeptics Online: Anonymity, Autonomy, and Discourse in a Hostile Environment, Berkman Center Research Publication No. 2015-2, 4 February 2015, https://ssrn.com/abstract=2560491 or http://dx.doi.org/10.2139/ssrn.2560491. Also the Egyptian LGBTQ community increasingly relies on encrypted communications such as Signal, https://www.alaraby.co.uk/english/indepth/2017/11/27/egypts-morality-police-get-on-grindr.

information — and promote 'the free flow of ideas and information' — without the risk of repercussions, disclosure, surveillance, or other improper conduct.[97]

Efforts to interfere with encryption are emerging as state trends

Despite its protective measures, unnecessary and disproportionate measures to undermine encryption have increased globally, threatening people's freedom of expression and security.[98] States have not provided evidence that such vulnerabilities were the least intrusive means of protecting national security, given the other tools at their disposal.[99] Experts say states must stop interfering with encryption unless they comply with international human rights law and adopt laws that protect encryption.[100]

Encryption 'backdoors' are irreconcilable with the principles of necessity and proportionality

Interferences with encryption tend to be presented as 'backdoors'. But even if deployed for legitimate purposes, they threaten the privacy necessary for exercising freedom of expression;[101] invariably affecting and undermining the security of all online users.[102] Weakening encryption for one, weakens it for all, and the collateral impact of a measure on persons not party to an application is relevant to the necessity and proportionality assessment, particularly if there are less intrusive measures available such as judicially authorized decryption of a device and judicial orders for the provision of a password.[103]

Lack of data available to understand the need for decryption based on the grounds of national security

Empirical data outlining the number of investigations and prosecutions that have been thwarted by encryption, and the rate of change of the same, is lacking.[104] In 2019, Europe, Europol and Eurojust reported that official statistics on how much digital evidence is seized in criminal investigations, or on the number of investigations that require decryption of data, are not available.[105] Follow-up reports in

---

[97] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, to the Human Rights Council, May, 2015, A/HRC/29/32 par. 6; *Delfi AS v Estonia* [2015] EMLR 26 at [147] and [149]

[98] Kaye, Ibid. Also in 2018, Kaye reported that the challenges faced by users had 'increased substantially' since 2015, highlighting how Pakistan had passed laws cracking down on the use of encryption; Iran banned encryption. See Research Paper 1/2018, June 2018, Encryption and Anonymity follow-up report, Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, par 2: https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf . Turkey arrested thousands of citizens for the alleged use of an encrypted messaging app, see Human Rights Council, U.N. Doc. April 2017. A/HRC/RES/34/7 par. 15. There is 'mounting' state pressure on companies to install encryption 'backdoors'. Ibid, par. 13; For a more detailed discussion about how backdoors undermine the security of all online users see PACE, Committee on Legal Affairs and Human Rights, Report

[99] Reference to traditional policing and intelligence and transnational cooperation, also wiretapping, geo-location and tracking, data-mining, traditional physical surveillance. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye to the Human Rights Council, March 2017. A/HRC/35/22, par. 21

[100] Human Rights Council, U.N. Doc. April 2017. A/HRC/RES/34/7 par. 9

[101] Ibid, par. 43

[102] Ibid, par. 42

[103] See *Voskuil v Netherlands* [2008] EMLR 14 at [65] and [71]

[104] Lewis, James; Zheng, Denise; Carter, William A. The Effect of Encryption on Lawful Access to Communications and Data. Center for Strategic and International Studies, February 2017, https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data p30

[105] Europol and Eurojust. First report of the observatory function on encryption, January 2019, https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2019-01_Joint-EP-EJ-Report_Observatory-Function-on-Encryption_EN.pdf

2020[106] and 2021[107] failed to provide such statistics with those reports simply noting encrypted communication was a 'recurring' issue.[108] Academics have also highlighted the lack of evidence to show the true extent of the problem.[109] This lack of empirical data — particularly in a 'golden age for surveillance'[110] — detracts from necessity arguments and consequently leaves proportionality analyses largely unsubstantiated, which chimes with the view that states often fail to provide public justification for restrictions or the need to breach encryption via backdoors.[111]

[106] Europol and Eurojust. Second report of the observatory function on encryption, February 2020, https://www.europol.europa.eu/cms/sites/default/files/documents/second_observatory_function_report.pdf
[107] Europol and Eurojust. Third report of the observatory function on encryption, July 2021, https://www.eurojust.europa.eu/third-report-observatory-function-encryption
[108] See p8 in 2020 report and p18 in 2021 report
[109] Ian Walden (2018). 'The Sky is Falling!' – Responses to the 'Going Dark' problem. Computer Law & Security Review. 34
[110] Jennifer Stisa Granick, If the Government Had Its Way, Everything Could be Wiretapped, ACLU, February 2019, https://www.aclu.org/blog/privacy-technology/internet-privacy/if-government-had-its-way-everything-could-be-wiretapped;
Peter Swire. The Golden Age of Surveillance, Slate, July 2015, https://slate.com/technology/2015/07/encryption-back-doors-arent-necessary-were-already-in-a-golden-age-of-surveillance.html
[111] Research Paper 1/2018, June 2018, Encryption and Anonymity follow-up report, Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf