Privacy International's response
to the call for input on the development of practical tools
to assist law enforcement bodies in promoting and protecting human rights
in the context of peaceful protests

05 April 2023

Introduction

Privacy International welcomes the opportunity to provide input to the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association on the tools and guidelines which may assist law enforcement in promoting and protecting human rights in the context of peaceful protests to be presented at the 55th session of the UN Human Rights Council.[1]

Privacy International (PI) is a non-governmental organisation that researches and advocates globally against government and corporate abuses of data and technology.[2] It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. PI has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development, the UN Office of the High Commissioner for Human Rights, and the UN Refugee Agency.

PI recognises the important role of law enforcement can play in facilitating the enjoyment of freedom of assembly. However, states need to ensure that any measures taken to do not undermine the

[1] UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, "Call for inputs: Development of practical tools to assist law enforcement bodies in promoting and protecting human rights in the context of peaceful protests, to be presented at the 55th session of the UN Human Rights Council", 7 April 2023 https://www.ohchr.org/en/calls-for-input/2023/call-inputs-development-practical-tools-assist-law-enforcement-bodies
[2] https://privacyinternational.org/

enjoyment of the very right they claim to protect. PI's submissions focus on how policing powers which enable law enforcement to undertake surveillance – before, during and after a protest – can be restrained through legislative and practical safeguards in order to ensure that states are meeting their positive obligation to facilitate assemblies. The following sections provide PI's information and analysis of some of the topics listed in the call for submission.

1. Protest surveillance as a direct interference with freedom of peaceful assembly

International human rights law recognises that law enforcement can play an important role in fulfilling states' positive obligation to facilitate and protect the right to freedom of peaceful assembly.[3] However, policing powers, including surveillance, enacted to facilitate assemblies must genuinely enable participation in protests and must be strictly limited in order to ensure they are not used to suppress protests or to justify excessive restrictions to these freedoms.[4]

The UN High Commissioner for Human rights has recognised this, concluding that "the use of [new] technologies to surveil or crack down on protesters [can lead to] … infringement of the right to peaceful assembly"[5] and this mandate has made it clear that, "the use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly and association, in both physical and digital spaces, should be prohibited."[6]

Protests surveillance is directly linked to numerous human rights abuses which were already raised in the Special Rapporteur's 2022 Report.[7] For example, reports have highlighted how specific tools deployed by the government in Iran in the recent wave of mass protests were used not only to supress unrest, but also to track and identify protesters, as well as access their private conversations.[8] In a context where dozens of people have been subjected to arbitrary arrests for protesting,[9] and a

[3] UN Human Rights Committee, General Comment No 37: On the right of peaceful assembly (article 21), 129th Session, adopted 17 September 2020, UN Doc CCPR/C/GC/37, para VI, https://undocs.org/CCPR/C/GC/37

[4] UN Human Rights Council, Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary, or arbitrary executions on the proper management of assemblies, 4 February 2016, UN Doc A/HRC/31/66, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/018/13/PDF/G1601813.pdf?OpenElement

[5] UN Human Rights Council, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, including Peaceful Protests: Report of the United Nations High Commissioner for Human Rights, 24 June 2020, UN Doc A/HRC/44/24, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/35/PDF/G2015435.pdf?OpenElement

[6] UN Human Rights Council, "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", (2019), UN Doc A/HRC/41/41, at para. 3, accessed online: https://undocs.org/A/HRC/41/41.

[7] UN Human Rights Council, "Protection of human rights in the context of peaceful protests during crisis situations", 16 May 2022, UN Doc A/HRC/50/42, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/343/05/PDF/G2234305.pdf?OpenElement

[8] Sam Biddle and Murtaza Hussain, "Hacked Documents: How Iran Can Track and Control Protesters' Phones", *The Intercept*, October 28 2022, https://theintercept.com/2022/10/28/iran-protests-phone-surveillance/

[9] David Gritten, "Iran protests: Ex-president's daughter jailed for five years – lawyer", *The BBC*, 10 January 2023, https://www.bbc.co.uk/news/world-middle-east-64220940

number have been sentenced to death[10], this type of surveillance has dire consequences for the right to freedom of assembly.

Further, in the context of mass uprisings, the existence of unrestrained and pervasive surveillance creates a genuine fear that protesters will be identified and targeted for exercising their rights. This was documented during the pro-democracy protests in Hong Kong in 2021.[11] Similar threats and attacks – which resulted from unlawful surveillance - against human rights defenders who documented police violence during the national strikes which took place in Colombia in 2021 have been reported.[12] In 2022, security forces in Egypt reportedly "arrested hundreds of people in downtown Cairo and town squares across Egyptian cities over content on their phones," and a number of them reported being questioned over their participation in online groups which were calling for protests ahead of Egypt hosting the COP27 conference.[13] Finally, a recent review by a Reuters reporter of more than 2,000 court cases showed how Russia uses facial recognition to identify, arrest, and prosecute peaceful protesters and political opponents.[14]

Powers and practices which enable law enforcement to undertake surveillance of protesters can violate states' positive obligation to facilitate and protect assemblies.[15] First, the use of certain surveillance tools such as, IMSI catchers[16], can be used not only to monitor and intercept ingoing and outgoing communications, but can also edit or reroute mobile communications, as well as block service. This can amount to a direct interference with freedom of assembly at the detriment of facilitating.

[10] Al Jazeera News Agencies, "Iran executions 'state sanctioned killing': UN rights chief", 10 January 2023, https://www.aljazeera.com/news/2023/1/10/iran-executions-amount-to-state-sanctioned-killing-un-says

[11] Shira Ovide, "The Real Dangers of Surveillance: What Americans can learn from the protests in Hong Kong", *The New York Times*, 12 June 2020, https://www.nytimes.com/2020/06/12/technology/surveillance-protests-hong-kong.html; See also, Human Rights Watch, "Hong Kong: Mass Arrests of Pro-Democracy Politicians", 8 January 2021, https://www.hrw.org/news/2021/01/08/hong-kong-mass-arrests-pro-democracy-politicians.

[12] Gimena Sànchez Garzoli, "The Repercussions of Confronting Police Abuses in Colombia, Killings Continue", *WOLA*, 23 December 2021, https://www.wola.org/2021/12/the-repercussions-of-confronting-police-abuses-in-colombia-killings-continue/

[13] Amnesty International, "Egypt: Arrests over calls for protest during COP27 expose reality of human rights crisis", November 6 2022, https://www.amnesty.org/en/latest/news/2022/11/egypt-arrests-over-calls-for-protests-during-cop27-expose-reality-of-human-rights-crisis/

[14] Lena Masri, "Facial recognition is helping Putin curb dissent with the aid of U.S. tech", 28 March 2023, *Reuters*, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions

[15] We use "protest surveillance" to refer to any type of overt or covert information gathering and/or intelligence gathering which includes the processing (such as analysis, use, and retention) of personal data about individuals who are exercising their right to protest, before, during, and after a protest, regardless of whether such protest takes place on the internet, in other virtual spaces or in physical spaces. For a full analysis of the legal limits that must apply to protest surveillance, see PI, "Restraining Protest Surveillance: when should surveillance of protesters become unlawful?", November 2022, https://privacyinternational.org/sites/default/files/2023-01/PI-RPS-sp-v7-RGB_no_blank.pdf

[16] There are devices typically collect International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) data that are unique to each mobile phone and SIM card – this is where they get one of their names, IMSI catchers. PI, IMSI catchers: PI's legal analysis, June 2020, https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis

Second, subjecting everyone who is involved in protest to mass surveillance erodes the right to freedom of assembly instead of facilitating it.[17] Generalised, and indiscriminate surveillance subjects anyone who wishes to participate in a protest to a variety of serious sanctions, and, ultimately, has a chilling effect on individual's and communities' ability to take collective action safely and freely. This impairs the enjoyment of the right to freedom of assembly, and as a result its essence.[18] Depending on the technologies being deployed, this means protesters may be subjected to what could ultimately be described as virtual stop-and-searches without limitations.[19]

Third, international courts and monitoring bodies have challenged the powers of the police to surveil individuals in public spaces and retain personal information about them just because they participated in peaceful assemblies. For instance, the European Court of Human Rights (ECHR) has concluded that the retention of the data of an activist, never being convicted of any offence, concerning their participation in peaceful protest had neither been shown to be generally necessary, nor necessary for the purposes of a particular inquiry.[20] Furthermore, such practices can further facilitate the potential persecution and criminalization of freedom of peaceful assembly.[21]

Similarly, where law enforcement agencies have the power to undermine the privacy of communications of certain protesters without appropriate justification or prior authorisation, such as a judicial warrant, surveillance powers can infringe on freedom of assembly. The UN Human Rights Council has recognised the importance of secure and private communications in the organisation and conduct of assemblies.[22]

Any legislation, guidance, or practice which enables law enforcement to undertake protest surveillance before, during or after a protest, is unlawful under international human rights law unless such powers are prescribed by law, and necessary and proportionate in the circumstances.[23]

---

[17] PI, "Restraining Protest Surveillance: when should surveillance of protesters become unlawful?", November 2022, pp 16–19, https://privacyinternational.org/sites/default/files/2023-01/PI-RPS-sp-v7-RGB_no_blank.pdf

[18] UN Human Rights Committee, General Comment No 31, "The Nature of the General Legal Obligation Imposed on States Parties to the Covenant", 26 May 2004, UN Doc CCPR/C/21/Rev.1/Add.13, para 6, https://digitallibrary.un.org/record/533996?ln=en

[19] PI, "Restraining Protest Surveillance: when should surveillance of protesters become unlawful?", November 2022, pp 16–19, https://privacyinternational.org/sites/default/files/2023-01/PI-RPS-sp-v7-RGB_no_blank.pdf

[20] PI, "*Catt v. the United Kingdom* - police powers to retain personal data in "extremism database" violates the rights of peace activist", January 2019, https://privacyinternational.org/news-analysis/2665/catt-v-united-kingdom-police-powers-retain-personal-data-extremism-database

[21] Lena Masri, "Facial recognition is helping Putin curb dissent with the aid of U.S. tech", 28 March 2023, *Reuters*, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions

[22] HRC, "The Promotion and Protection of Human Rights in the Context of Peaceful Protests", HRC Res 44/20, 17 July 2020, https://documents-dds-ny.un.org/doc/UNDOC/LTD/G20/178/26/PDF/G2017826.pdf?OpenElement

[23] For further analysis on protest surveillance as a direct interference with the right to freedom of assembly, see, Ilia Siatitsa, "Freedom of assembly under attack: General and indiscriminate surveillance and interference with internet communications", (2020) 102 (913) *International Review of the Red Cross* 181-198.

2. PI's recommendations regarding laws, guidance, protocols and mechanisms or strategies/practices related to the facilitation and policing of protests

PI urges the UN Special Rapporteur to include in their report the following recommendations that should apply to surveillance undertaken by law enforcement at every stage of a protest:

a. **Indiscriminate and generalised protest surveillance is unlawful.**

b. **Any power to undertake targeted protest surveillance should adhere to requirements under international human rights law**: is based on a clear, accessible, and transparent legal basis; it is targeted at a specific individual, is necessary in a democratic society to achieve the legitimate aims outlined within the rights to privacy and freedom of assembly; is the least intrusive means by which that legitimate aim can be achieved, both in the context of the right to privacy and freedom of assembly (i.e. the impact of the targeted surveillance on the right to privacy and freedom of peaceful assembly is proportionate to the legitimate aim being pursued); and there are appropriate and robust safeguards in place).

c. **Any power to undertake protest surveillance must be subjected to clear restrictions and robust safeguards**. This includes information security safeguards (including encryption of audio-visual footage collected at protests), access limitation and warrant-based access, limits on retention, effective oversight mechanisms, and effective and accessible mechanisms for protesters and organisations to challenge any form of surveillance they are exposed to.

d. **Facial recognition technologies** should never be used to identify those peacefully participating in protests. As the UN High Commissioner for Human Rights has recommended that States "[n]ever use facial recognition technology to identify those peacefully participating in an assembly".[24]

[24] An important legal case which highlights the significance of the legal safeguards outlined above, at paras. 2.3 – 2.5 is *Bridges* v *South Wales Police*. The UK Court of Appeal held that a police force's deployment of automated facial recognition technology (AFRT) was not "in accordance with the law", particularly because the police powers to deploy the technology (who was it going to be deployed against and where it would be deployed) was left to the discretion of individual police officers. As a result, the polices' use of AFRT was found to be a violation of the applicant's right to privacy under Article 8 of the European Convention on Human Rights. *R (on the application of Edward Bridges)* v *South Wales Police* [2020] EWCA Civ 1058, paras 81–94, https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

e. States must ensure that before any surveillance technologies are acquired by law enforcement agencies, they are subjected to **prior human rights impact assessments**.

In a recent decision, the European Ombudsman[25] issued a decision which concluded that the European Commission had failed to take necessary measures to ensure the protection of human rights in the transfers of technology providing support to third countries to develop surveillance capabilities.[26] The decision specifically recommended that the Commission now requires an "assessment of the potential human rights impact of projects be presented together with corresponding mitigation measures."[27] The lack of such protections, which the Ombudsman called a "serious shortcoming", poses a clear risk that these surveillance technologies might cause serious violations of or interferences with other fundamental rights.

3. Measures to prevent and minimise harms

Safeguards against generalised and indiscriminate data retention: PI submits that in the absence of individualised reasonable suspicion, it is unlawful to retain protesters' personal data merely because they participated in a protest. Any personal data collected incidentally must be deleted without undue delay. This policy would minimise the harm which stems from the databases being built about journalists and human rights defenders who regularly participate in monitoring protests.

For example, in *Catt v the UK* the European Court of Human Rights (ECtHR) held that the UK had violated Catt's rights under Article 8 of the ECHR, because authorities retained the applicants' data just because they had participated in protests.[28] The ECtHR further emphasised that:

> [T]he absence of effective safeguards was of particular concern in the present case as personal data revealing political opinions attracts a heightened level of protection. **Engaging in peaceful protests has specific protection under Article 11 of the Convention**...[29]

Safeguards against mobile phone extraction and other intrusive practices: Secondly, PI has undertaken extensive research uncovering the intrusive nature of mobile phone extraction

[25] The EU oversight body responsible for ensuring that EU agencies comply with legal obligations.
[26] PI, "EU Watchdog Finds Commission Failed to Protect Human Rights From its Surveillance Aid to African Countries", 5 December 2022, https://privacyinternational.org/press-release/4992/eu-watchdog-finds-commission-failed-protect-human-rights-its-surveillance-aid
[27] PI, "EU Watchdog Finds Commission Failed to Protect Human Rights From its Surveillance Aid to African Countries", 5 December 2022, https://privacyinternational.org/press-release/4992/eu-watchdog-finds-commission-failed-protect-human-rights-its-surveillance-aid
[28] ECtHR, *Catt* v *the United Kingdom* (App no 43514/15), 24 January 2019, para 119.
[29] *ibid,* para 123 (emphasis added).

technology[30], especially in the context of protests.[31] In the absence of robust safeguards which prevent law enforcement from gathering unlimited amounts of data from detainees electronic devices, anyone who participates in an assembly, including lawyers, journalists and human rights defenders may be subjected to unlawful collection and retention of private and sensitive information simply as a result of exercising their fundamental rights. For example, PI's partners in Lebanon have documented device seizures by security agencies across a number of protests between 2015 and 2019 as part of a wider crackdown on freedom of expression and assembly.[32] During this period, lawyers, activists, and protesters pushed for law enforcement to follow the law requiring officers to ensure that detainees have access to a lawyer while in police custody. The right to legal counsel made a significant difference to protesters' understanding of their rights, and their ability to respond during interviews without feeling as though they were under duress.[33]

PI recommends that, in the aftermath of a protest, where law enforcement have undertaken arrests of protesters or detained individuals who have participated in protests, it is crucial that:

i. Law enforcement agencies obtain a warrant before undertaking any searches of electronic property; and
ii. Detainees have access to legal advice through the attendance of a lawyer wherever they are detained before any interview takes place and before they submit any evidence to law enforcement agents.

4. Measures to facilitate the exercise of the right to freedom of peaceful assembly and protect the rights of groups particularly at risk in the context of protests

Prohibiting discriminatory surveillance practices: It must be unlawful to undertake any form of protest surveillance on the basis of race, ethnicity, sex, religion, political or other opinion, national or social origin, association with a national minority, property, birth, or other status.[34]

[30] PI, "Digital Stop and Search: How the UK police can secretly download everything from your mobile phone", 27 March 2018, https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile; See also, PI's Complaint to the UK Information Commissioner's Office RE: Digital Stop and Search, 26 April 2018, https://privacyinternational.org/sites/default/files/2018-04/Complaint%20to%20ICO%20about%20Mobile%20Phone%20Extraction%2026th%20April%202018.pdf

[31] PI, "How mobile phone extraction can be used at a protest", 21 April 2021, https://privacyinternational.org/explainer/4484/how-mobile-phone-extraction-can-be-used-protest

[32] SMEX, "Device Seizures in Lebanon", January 2021, https://smex.org/wp-content/uploads/2021/02/SMEX-Device-Seizures-Report-2021-eng.pdf

[33] Ghida Frangieh, "Lebanese Uprising Enshrines Defense Rights for Detainees", Legal Agenda, 30 November 2020, https://english.legal-agenda.com/lebanese-uprising-enshrines-defense-rights-for-detainees/

[34] For further research around ethnic minorities being placed at risk of heightened surveillance and therefore interferences with their fundamental human rights, see, PI, "Ethnic minorities at greater risk of oversurveillance after protests", 15 June 2020, https://privacyinternational.org/news-analysis/3926/ethnic-minorities-greater-risk-oversurveillance-after-protests

When deciding whether or not to participate in a protest, people around the world often "rely on the anonymity of the crowd to protect themselves against retribution, particularly in contexts where any form of dissent is suppressed."[35] This allows people and groups to freely express their views without fear of being identified and targeted for reprisal. Every person has the right to freedom of assembly, and it is unlawful for states to impose restrictions which are either directly or indirectly discriminatory on the basis of race, sex, religion, political opinion, or nationality.

For example, a person with temporary or irregular migration status should have the right to protest anonymously, without fear that their attendance at a protest will be recorded and shared with law enforcement or other agencies making decisions about their right to remain in a given country. Additionally, if an individual wants to attend a protest in support of LGBT+ rights but does not want a 'record' of their presence at a protest for personal reasons, they have a reasonable expectation that the privacy of their identity (that is, their anonymity) will be maintained.

Banning predictive policing technologies: Further, predictive policing technologies intended to gather generalised data should never be deployed during protests. Additionally, predictive policing cannot be used as a blanket justification by police and/or law enforcement to collect and retain personal data about protesters without limitation. Predictive policing is best understood as a form of "further processing" after law enforcement have built up databases about activists or people who have attended a protest. Predictive policing relies on programs which work "by feeding historic policing data through computer algorithms."[36] PI has previously highlighted that, depending on the historic data that the police are using, these tools can be "incomplete or biased, leading to a 'feedback loop' sending officers to communities that are already unfairly over-policed".[37]

Public consultations before acquiring new technologies: Finally, PI recommends that in before law enforcement agencies acquire and deploy new technologies which ostensibly assist agents in facilitating and policing assemblies, the relevant authorities must undertake proactive, transparent consultations which engage both the public and civil society. Consultations must give members of the public a meaningful opportunity to respond, particularly where certain technologies are likely to have a higher impact on specific communities. For example, when the Metropolitan Police Service in the

[35] Ilia Siatitsa, "Freedom of assembly under attack: General and indiscriminate surveillance and interference with internet communications", (2020) 102 (913) *International Review of the Red Cross* 181-198, p 194.
[36] See for example, evidence from interviews with senior police in the UK in, Lina Dencik, Arne Hintz and Zoe Carey, "Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom", (2018) 20(4) *New Media and Society* 1443-1540, p 1440.
[37] PI, "How predictive policing can be used at protests", 5 May 2021, https://privacyinternational.org/explainer/4501/how-predictive-policing-can-be-used-protests

United Kingdom started to deploy facial recognition technology (FRT) in public spaces and during public events, there were reportedly "no clear, proactive processes for the public, especially marginalised communities, to influence if and how FRT was implemented."[38] This is significant firstly, because of the proven biases built into FRT,[39] but secondly, it undermines the concept of 'policing by consent', which is central to the effective facilitation of peaceful assemblies.[40]

5. Measures for supporting accountability for human rights violations in the context of protests

Notification of victims of surveillance: Whenever a relevant authority exercises a power to undertake targeted protest surveillance, such authority must be under an obligation to inform and/or notify each individual that their personal data has been collected as a result of targeted protest surveillance without undue delay following the end of any criminal investigation. Any notification must be accompanied by an effective and exercisable right for individuals and/or organisations to challenge the lawfulness of protest surveillance and to seek remedies for unlawful protest surveillance.

Safeguards for public-private surveillance partnerships: Additionally, where law enforcement agencies are empowered to enter contractual relationships with private companies for the provision of tools and technologies intended to facilitate assemblies (for example, the provision of drones to police forces for use during protests)[41] there should be clear, transparent guidelines which impost limits on these types of partnerships. PI argues that there are six basic safeguards that should be considered whenever a public entity enters into a partnership with a private company (transparency, adequate procurement, accountability, legality, necessity and proportionality, oversight, and redress).[42]

The role of civil society in ensuring authorities are held accountable for abuses in times of crisis or other: Civil society has a key role in ensuring accountability for law enforcement officials alleged of committing human rights violations in the context of protests. This is exemplified by their role during the Covid-19 pandemic. Throughout the pandemic, civil society organizations have played an important role as watchdogs monitoring the ongoing crisis and documenting the impacts of Covid-19

[38] Evani Radiya-Dixit, "A Socio-technical audit assessing police use of facial recognition technology," Minderoo Centre for Technology and Democracy, October 2022, p 134, https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf
[39] Alex Najibi, "Racial Discrimination in Face Recognition Technology" 24 October 2020, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/; See also, Michael Gentzel, "Biased Face Recognition Technology Used by Government: A problem for liberal democracy", (2021) 34 *Philosophy and Technology*, pp 1639-1663.
[40] See, for example, Liz Gorny, "We Do Not Consent examines increased police powers over lockdown through 27 protests", *Its Nice That,* 13 June 2022, https://www.itsnicethat.com/news/jeremy-jeffs-we-do-not-consent-photography-130622
[41] Vikram Dodd, "Drones used by police to monitor political protests in England", *The Guardian*, 14 February 2021, https://www.theguardian.com/uk-news/2021/feb/14/drones-police-england-monitor-political-protests-blm-extinction-rebellion
[42] PI, "Safeguards for Public-Private Partnerships", December 2021, https://privacyinternational.org/sites/default/files/2021-12/PI%20PPP%20Safeguards%20%5BFINAL%20DRAFT%2007.12.21%5D.pdf

surveillance measures on human rights and fundamental freedoms. In a recent report, ECNL, INCLO, and PI[43] highlight a few indicative examples of strategic litigation efforts and other advocacy campaigns led by civil society to resist unlawful surveillance in and of their communities. Among others:

- In France, May 2020, two civil society organisations, La Quadrature du Net (LQDN) and La Ligue des Droits de l'Homme, filed a successful lawsuit to block the use of drones to enforce Covid-19 lockdown in Paris.

- In Colombia, a challenge by journalists and others with the support of civil society, including Dejusticia,[44] reinforced the obligation to respect the right to privacy even during a national state of emergency.[45]

- In Israel, the Association for Civil Rights in Israel (ACRI) submitted a successful petition to the High Court of Justice, that found that Shin Bet was "not constitutionally authorized to collect, process and use 'technological information'" of Covid-19 patients.[46]

[43] PI, ECNL, INCLO, "Under Surveillance: (Mis)use of Technologies in Emergency Responses Global lessons from the Covid-19 pandemic" (2022) https://privacyinternational.org/sites/default/files/2022-12/ECNL%2C%20INCLO%2C%20PI-COVID-19-Report-Final.pdf In collaboration with Daniel Ospina Celis, Lucia Camacho, Juan Carlos Upegui (Dejusticia in Colombia), Bastien Le Querrec (La Quadrature du Net in France), Amber Sinha (Policy in India), Nadine Sherani, Rozy Sodik, Auliya Rayyan (KontraS in Indonesia), Martin Mavenjina (Kenya Human Rights Commission in Kenya), Sherylle Dass, Devon Turner (Legal Resources Centre in South Africa).

[44] Dejusticia, "Lack of transparency around contact-tracing app" in: PI, ECNL, INCLO, "Under Surveillance: (Mis)use of Technologies in Emergency Responses Global lessons from the Covid-19 pandemic" (2022) https://privacyinternational.org/sites/default/files/2022-12/ECNL%2C%20INCLO%2C%20PI-COVID-19-Report-Final.pdf

[45] See also Karisma, "CoronApp, Medellín me Cuida y CaliValle Corona al laboratorio -O cómo se hackea CoronApp sin siquiera intentarlo-" (2020) https://web.karisma.org.co/coronapp-medellin-me-cuida-y-calivalle-corona-al-laboratorio-o-como-se-hackea-coronapp-sin-siquiera-intentarlo/

[46] The Association for Civil Rights in Israel, The Association for Civil Rights in Israel, "*We Won: HCJ Sides with ACRI Petition Against Shin Bet Tracking Civilians*" (2020) https://www.english.acri.org.il/post/__154; The Association for Civil Rights in Israel, "*GSS Tracking as a Part of the Struggle Against Corona – Fifth Petition"* (2021) https://www.english.acri.org.il/post/__385