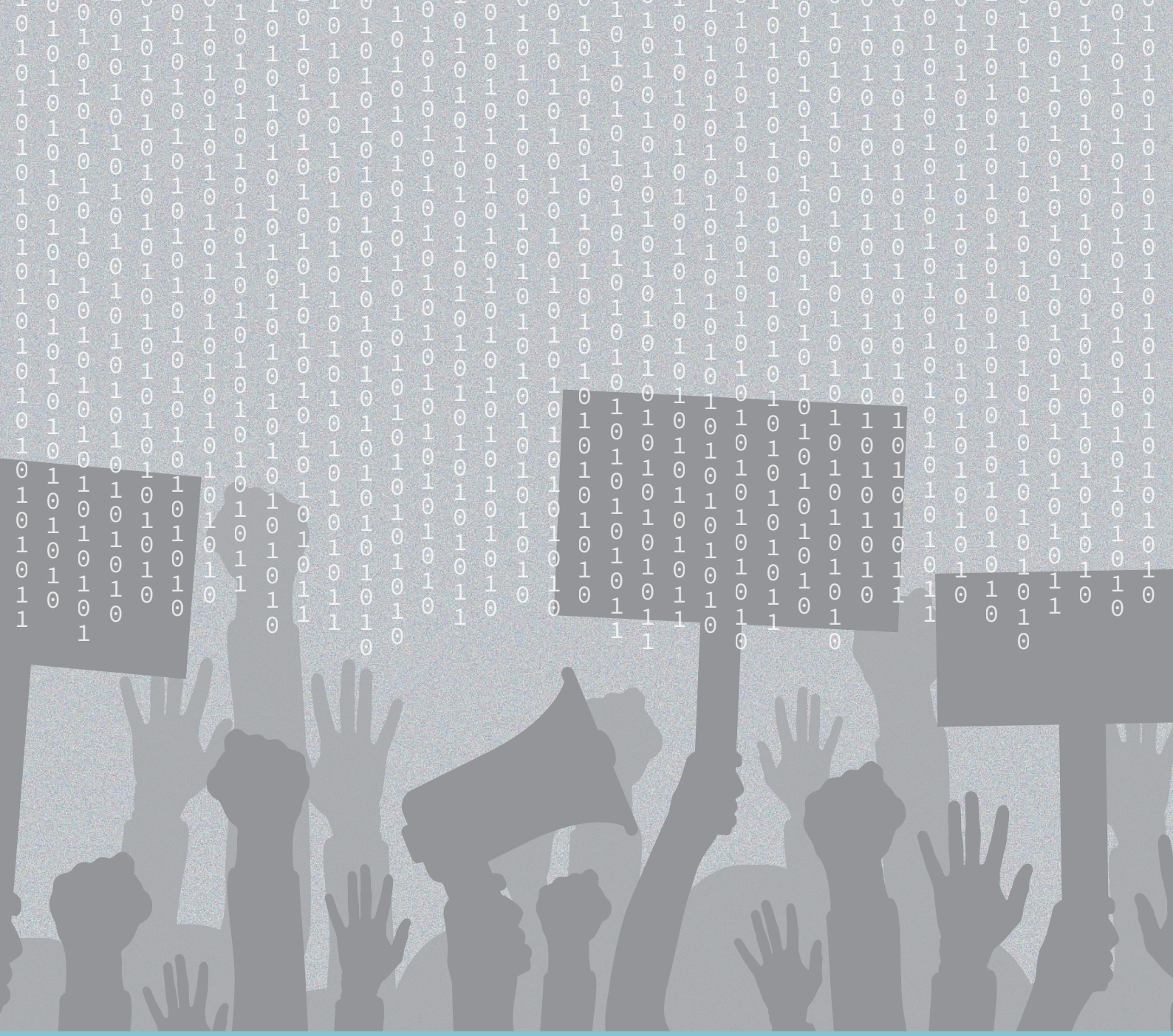

SPYING ON DISSENT

SURVEILLANCE TECHNOLOGIES AND PROTEST

INCLO
INTERNATIONAL NETWORK OF CIVIL LIBERTIES ORGANIZATIONS

JUNE 2019

Acknowledgements

This INCLO report was drafted under the care of lead author and editor, Elizabeth Farries (INCLO).

This is a collaborative effort by 12 INCLO organisations. For their contributions of case studies, research, drafting and/or criteria for international recommendations, INCLO sincerely thanks: Lucila Santos (INCLO); Damir Gainutdinov (Agora); Jamil Dakwar and Jennifer Turner (ACLU); Avner Pinchuck and Anne Suciu (ACRI); Rob De Luca (CCLA); Marcela Perelman and Margarita Trovato (CELS); Vivian Newman Pont and María Paula Ángel (Dejusticia); Szabolcs Hegyi (HCLU); Martin Mavenjina (KHRC); Sherilyn Naidoo (LRC); and Hannah Couchman, Gracie Bradley, and Corey Stoughton (Liberty).

INCLO credits Taryn McKay for design and photo editing and Hilary Burke for copyediting.

Table of Contents

Overview

Protest under threat

The ability to publicly express beliefs and opinions and to associate is essential to democracy[1]. Protests[2] are a central tool of public expression and engagement, often serving as the only avenue for advocacy seeking political, social or economic reforms. Despite the importance of protest to a free society, many states have failed to adequately protect protest and public speech. In fact, policing institutions overwhelmingly treat protests as security threats that should be discouraged and suppressed.

New threat to protest: online surveillance technologies

Although protest rights are mainly understood in the context of physical gatherings, human rights protections should also apply to 'analogous interactions taking place online.'[3] In this context, many challenges to the protection against unlawful interference with our rights to online and offline protest have materialised in this digital age. Recent years have seen a sharp expansion of **online surveillance technologies by policing institutions**[4] **against protests and protesters**[5]**, and association**[6]. These technologies are designed or used to watch, intercept, record, retain, analyse and disseminate personal data about

[1] For more information about the rights attached to protest see INCLO's 2018 report *Defending Dissent*, available at: https://www.inclo.net/pdf/Defending-Dissent-Report-Complete-WEB-FINAL.pdf

[2] INCLO's use of the term 'protest' follows that of the Joint Report of the Special Rapporteur together with the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions on the Proper Management of Assemblies: A protest is 'an intentional and temporary gathering in a private or public space for a specific purpose, and can take the form of demonstrations, meetings, strikes, processions, rallies or sit-ins with the purpose of voicing grievances and aspirations or facilitating celebrations.' See UN Doc. A/HRC/31/66 (4 February 2016), para. 10.

[3] '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', UN Doc. A/HRC/31/66 (4 February 2016), para. 10.

[4] The term 'policing institutions' comes from our *Defending Dissent* report and represents those state agencies and law enforcement agents (excluding non-state actors) tasked with the responsibility for safety, security and the protection and promotion of the rights to protest. Available at: https://www.inclo.net/pdf/Defending-Dissent-Report-Complete-WEB-FINAL.pdf. However, we also point out that the use of these technologies is not exclusive to police or other government institutions tasked with the responsibility for safety or security. For example, intelligence agencies and the judiciary conduct surveillance, often with no acknowledgment of or compliance with due process and guarantees. Further, as the Association for Civil Rights in Israel elaborates at footnotes 65 and 66, private social media companies also have surveillance and authoritative policing powers that compare with states.

[5] Those activists, organisers and individuals or groups who participate in protests.

[6] However, in raising awareness about these specific sets of rights captured by the Special Rapporteur's mandate, we must clarify at the outset that our discussion here in relation to these rights **does not** imply lower standards for other individuals' rights and freedoms.

protesters – often without our knowledge, our consent, without real and effective oversight and control, and without available legal avenues of recourse. This can disrupt and preclude our freedom and ability to organise, gather, dissent and assemble.

Protest online: the continuity and interplay with offline spaces

When we consider how protest manifests in our digital age, we acknowledge that creating distinctions between online and offline protest tend to blur the continuum. Laws applied in offline spaces impact behaviour in online spaces, and policing institution actions in online spaces can have offline consequences. For example, policing institutions follow people who organise protest activities or are just involved in certain networks on social media and intercept their online communications. They film protesters and use face surveillance, upload details into online databases, and use evidence of online protest activity for criminal and administrative prosecutions and convictions. **Therefore, rather than engaging in the legally complex challenge of separating and defining the concept of 'online' protest in distinction to its offline counterpart, we instead identify the types of online surveillance technologies used to deter protesters' rights, in online and offline spaces alike.**

Lack of democratic engagement or human rights safeguards

INCLO's case studies from 13 countries demonstrate that the way policing institutions select and deploy online surveillance technologies against protesters often occurs without necessary human rights and democratic safeguards. There is often no clearly defined legal framework specifying when and how these tools can be used, no limits or safeguards for fundamental freedoms and individual rights, and no due regard for whether deployment is compatible with human rights protections. There is no clarity about judicial requirements or instances for judicial review. The governing rules and practices are not transparent; there is no publicity or information about police and security institutions' use and no clear way of accessing this information. There are insufficient mechanisms for overseeing these institutions' operations, as well as limited avenues for pursuing accountability and redress when these surveillance tools are used in ways that are not compatible with fundamental rights.

Part 1. Online surveillance technologies used to limit protest

Given that access to information laws often exempt policing institutions,[7] it can be very difficult to identify and track the ways in which these institutions deploy online surveillance technologies against protesters. However, as our INCLO members' case studies reveal, we know or strongly suspect that these technologies are applied in various forms in all of our countries. The types of surveillance deployed can be categorised as follows:

1.1 Watching online protest activity via social media networks

Social media networks are a widely available and well-used resource for organising or responding to calls to participate in protest actions. They are also used as an information source by policing institutions and so are sometimes described as 'open sourced intelligence.' It is increasingly common for policing institutions to receive state training on how to engage protesters and track their online activities.[8]

In INCLO member countries, policing institutions' use of social media in this way has interfered with people's ability to actively protest or has led to significant legal consequences.

> **In Russia, the Agora International Human Rights Group (Agora)** explains that policing institutions scan social media networks for protest activity. Police register accounts on social media networks, join various protest groups, and 'friend' civic activists in order to watch and document online posts.[9] As a rule, this police surveillance is aimed at collecting evidence to build administrative and criminal cases against the activists being watched. In such cases, screenshots from social networks have become staple building blocks in the body of state evidence.
>
> **In Israel, the Association for Civil Rights in Israel (ACRI)** writes that the Immigration Authority and the Ministry for Strategic Affairs use a variety of sources to identify alleged Boycott, Divestment and Sanctions (BDS)[10]

[7] See INCLO's efforts regarding intelligence sharing: https://www.inclo.net/pdf/iisp/unanswered_questions.pdf. Many of our requests were rejected outright, often due to statutory exemptions, while other entities

[8] See for example Miami-Dade Police Department, 'Advanced Social Media and Open Source Intelligence Research and Investigations', available at: http://events.r20.constantcontact.com/register/event?oeidk=a07eftx8fdfa1d5692f&llr=986tj7mab

[9] See for example the courtroom testimony of this police agent who 'friended' a group of activists and was included by them in their mailing list (*MediaZona*). Available in Russian at: https://zona.media/chronicle/delo_sokolova#9597

[10] The Boycott, Divestment and Sanctions movement (also known as BDS) is a global campaign promoting various forms of boycott against Israel.

activists, including social media. For example, the Ministry watched the social media posts of Lara Alqasem, a 22 year old American student and former president of a local chapter of the pro-boycott group Students for Justice in Palestine. Despite not participating in the boycott movement for years and also holding a valid entry visa, the state alleged that Alqasem continued to support the movement and so denied her entry. They cited as evidence the fact that Alqasem had recently deleted all of her social media accounts.

In Argentina, the Centro de Estudios Legales y Sociales (CELS) describes how two people arriving in Buenos Aires as intended civil society representatives at the World Trade Organization (WTO) Ministerial Conference were deported. They were among 65 people from civil society organisations throughout the world whose WTO accreditation had been rejected by Argentine security authorities 'for unspecified reasons'.[11] In response to the controversy over the rejected accreditations, a Foreign Affairs Ministry press release justified the decision on the grounds that the organisations or their members 'had made explicit calls via social media for violent demonstrations, expressing their intent to generate intimidation and chaos.'[12] Clearly, the Argentine government had been gathering intelligence, very possibly based on people's organisational affiliation or political opinion – which is expressly prohibited under Argentine law.[13]

In Egypt, the Egyptian Initiative for Personal Rights (EIPR), confirms that anti-protest laws implemented in offline space affect the ability of citizens to protest online, citing the experience of Alaa AAbdel Fattah. Alaa was arrested violently in 2013 after the government passed Law No. 107 banning street protests.[14] He was charged for organising a gathering of more than five individuals that was likely to endanger public order. A report from the Directorate of Information and Documentation showed that Alaa AAbdel Fattah used Twitter to ask people to demonstrate at the entrance to the Shura Council building.[15] The prosecution files and the

[11] On 9 December 2017, at a court hearing on a habeas corpus that was filed, the Argentine government presented the list of 65 people whose accreditations were rejected.
[12] Press release available at: https://cancilleria.gob.ar/es/actualidad/comunicados/sobre-la-acreditacion-de-ongs-la-conferencia-ministerial-de-la-omc-en-buenos
[13] Article 4 of National Intelligence Law 25.520, as modified by Law 27.126
[14] Alaa was finally released in 2019! For more information on the details attached to his arrest, see Wafa Ben Hassine, 'The Crime of Speech: How Arab Governments Use the Law to Silence Expression Online': https://www.eff.org/files/2016/04/28/crime-of-speech.pdf
[15] See Opinion No. 6/2016 adopted by the UN Working Group on Arbitrary Detention (6 June 2016): https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session75/Opinion_2016_6_Egypt.pdf

court ruling in the case brought against Alaa and others also referred to Alaa's use of his personal page on Facebook.

In India, the state has wavered on how broadly to deploy its powers in its mass surveillance project. Online, it focuses on sentiment analysis to watch publicly discussed issues and track matters relating to public order including 'sensitive issues and protests.'[16] This technology sorts online statements and content into categories which are 'positive' or 'negative' and which also create alerts to authorities depending on the criteria they have designed.[17]

In Hungary, the Hungarian Civil Liberties Union (HCLU) has growing evidence that the police, bolstered by the new assembly law effective since October 2018, have started to watch social media for when people organise or make public calls for protest. The new law now requires that protest organisers notify the police before even putting out a call to action, rather than simply informing police of the action date itself.[18] The police, relying on the strength of this law, now have the power to automatically sanction online protest organisers if they notify police of their intended action *after* making a public call for support.

In Kenya, the Kenya Human Rights Commission (KHRC) reports that human rights defenders and civil society organisations tend to rely on social media platforms like WhatsApp and email to organise advocacy and peaceful demonstrations on the streets of Nairobi and in other parts of Kenya. These platforms are vulnerable to unlawful surveillance by state agencies. This could explain why most of these peaceful demonstrations have been forcefully disrupted by officers from the National Police Service.

Operational assistance from social media

In addition to passively facilitating spying by policing institutions on protesters, we have evidence that social media companies are being compelled to exchange information with these institutions. We are also seeing examples of how social media companies are refusing to publish protest ads.

In Russia, Agora observes that law enforcement authorities have organised information exchanges with most of the social networks functioning under Russia's jurisdiction.[19] Authorities are able to obtain

[16] Amber Sinha of The Centre for Internet and Society, India, 'Social Media Monitoring', available at: https://cis-india.org/internet-governance/blog/social-media-monitoring
[17] Amber Sinha of The Centre for Internet and Society, India, 'Social Media Monitoring', available at: https://cis-india.org/internet-governance/blog/social-media-monitoring
[18] Act LV of 2018 on the right to assembly, Article 10, section 1. See more in 'Summary of the Hungarian Civil Liberties Union's Analysis of the New Bill on the Right to Assembly', available at: https://hclu.hu/en/articles/summary-of-the-hungarian-civil-liberties-unions-analysis-of-the-new-bill-on-the-right-to-assembly
[19] See for example social media sites including Vkontakte, Odnoklassniki and Moy Mir.

user IP addresses and subsequently identify the users' details: telephone number, residential address, etc.

In Israel, ACRI says that Facebook has denied them the opportunity to run ads on their English Facebook page that protest incidents of racism and the new 'nation-state law' in Israel. Facebook deemed their content too political.[20]

In the United States, the ACLU went to court to block the enforcement of search warrants targeting three Facebook accounts as part of the government's investigation and prosecution of activists arrested on Inauguration Day 2017 in Washington DC.[21]

1.2 Recording, face surveillance and protester databases

Filming and image capture, a traditionally 'offline' surveillance technique, now has an online presence. It can be subject to further algorithmic analysis including face surveillance, and also used to build prosecution evidence. In addition, captured footage is being stored in searchable databases. This sometimes occurs without cause (i.e. a formal investigation), sometimes when protesters are detained (but not convicted), and sometimes when protesters have been convicted.

In Russia, Agora explains that policing institutions capture protesters' images and add them to activist watchlist databases to help future identification. Authorities are using a mobile biometric complex with an NtechLab facial recognition system at mass protests. Anti-corruption demonstrators are among those on watchlist databases, and they have been compelled to visit police stations regularly for 'conversations'.[22] The database details are also used as evidence for prosecution. The police build the databases partly with information from general citizen databases, which record all citizen encounters with the police along with data on their modes of public transport.

In Canada, the Canadian Civil Liberties Association (CCLA) describes how during the 2018 York University protests supporting a local union strike, the university hired private security officers to supplement its

[20] The following explanation as given to ACRI by Facebook: 'Your ad was not approved because your Page has not been authorised to run ads with political content.'
[21] ACLU, 'ACLU-DC seeks protection for personal Facebook accounts against Inauguration Day search warrants' (28 September 2017) available at: https://www.aclu.org/news/aclu-dc-seeks-protection-personal-facebook-accounts-against-inauguration-day-search-warrants-0
[22] See for example the case of Andrei Chupyshev Maria Klimova. '"We will spend the night at your door": Activist from Krasnodar was put on a police watchlist because of participation in the March 26 rally'. (*MediaZona*, 24 April 2017) available in Russian at: https://zona.media/article/2017/24/04/profuchet

campus police force.[23] Protesters were regularly filmed throughout the strike via surveillance cameras.[24]

In Hungary, the HCLU observes how police recording of protests became a general practice after police abuses during the fall 2006 riots. Further, police have recently begun to use temporarily installed CCTV cameras. A recommendation was enacted by the parliamentary commissioner for data protection[25] that police delete recorded footage if they determine that the protesters were not violating laws. However, the HCLU has no information about whether the police are meeting this requirement to delete footage. The Hungarian National Authority for Data Protection and Freedom of Information puts out annual reports which reveal that it hasn't yet examined the police practice in this regard.[26] The HCLU suspects the police are instead retaining the footage and comparing it with other footage that the police capture of protesters who demonstrate outside the confines of the restrictive assembly law.

In the United Kingdom, Liberty describes how police forces are using face surveillance in live public settings.[27] Couched in deceptively neutral terminology like 'facial recognition', face surveillance technology is capable of identifying or verifying a person from a digital or video image or source. It can scan the faces of all passers-by in real time. The technology measures biometric facial characteristics, creating unique facial maps in the form of numerical codes. These codes are then compared with those of other images on databases, which are not limited to people wanted for crimes. Liberty describes how UK police are compiling their face surveillance data from live public settings in bespoke watchlists that include those not accused of crimes.

1.3 Hacking

Policing institutions are increasingly using devices capable of hacking into and watching our online protest communications on our ordinary devices, including phones and tablets. These police hacking tools can track our locations, who we

[23] CCLA, 'Preliminary Report on Rights Violations at York U - Survey Results' (29 March 2018) available at: https://ccla.org/yorku-strike-survey-results/
[24] A.T. Kingsmith, 'Strike Surveillance' (*Briarpatch Magazine*, 29 October 2018) available at: https://briarpatchmagazine.com/articles/view/strike-surveillance
[25] Recommendation 118/A/1995
[26] This body's annual reports are available at: https://www.naih.hu/annual-reports.html
[27] For example, at Remembrance Sunday commemorations in London in November 2017, the Metropolitan Police (the Met) compiled a watchlist of images of people with known mental health issues. The South Wales Police (SWP) and the Met have also admitted that images could come from social media.

talk to, what online information we are interested in, and even the content of our conversations, all without our knowledge or consent.

The SORM system

In Russia, the 'System for Operative Investigative Activities' (known as SORM) is the technical foundation for targeted mass communication surveillance. Communications service providers are obliged to install at their own expense a special device ('Punkt Upravlenia') on their networks that allows the Federal Security Service (FSB) to directly collect traffic without the knowledge or co-operation of the service provider. The FSB tracks behaviours including credit card transactions and other web use including social networks, chats and forums.

> **In Russia, Agora** describes repeated indirect indications of data use in Russia for covert surveillance of protesters' online activities.[28] Police often intercept activists at the places they frequent (cinemas, cafés, etc), even when the activists have not revealed their location.

IMSI catchers

Often described as 'stingrays' or 'grabbers', IMSI catchers are a class of surveillance devices that provide active online interception capabilities. Citizenlab calls them 'cell site simulators'[29] and says they mimic the strongest nearby cell phone tower to which our personal communications devices, including our mobile phones, connect. This connection allows the IMSI catchers to obtain identifiers that policing institutions use to secretly watch how we operate our personal devices.

> **In the United States, the ACLU** investigation into Florida police use of IMSI catchers did not produce any policies or guidelines governing the use of stingrays or restricting how and when they could be deployed, suggesting a lack of internal oversight.[30] The ACLU did discover however that the state has a troubling history when it comes to stingrays: according to a document available online but not among the records provided to the ACLU, the Miami-Dade Police Department first purchased a cell

[28] For example, on 20 January 2019 a public prosecutor came to the informal meeting of 'Open Russia' activists at the city café in Cheboksary and handed the subpoena to Yuriy Sidorov. See his personal Facebook account (20 January 2019) available in Russian at: https://m.facebook.com/story.php?story_fbid=2263701970584620&id=100008345174557

[29] Citizenlab definition (and discussion of the problem in Canada): a class of surveillance devices called 'cell site simulators', and which are commonly referred to as 'IMSI Catchers', 'Digital Analyzers', 'cell grabbers', and 'mobile device identifiers' or by brand names such as 'Stingray', DRTBOX and 'Hailstorm'. See: https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf

[30] ACLU, 'ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida' (22 February 2015) available at: https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida

site simulator in 2003 to surveil protesters at a Free Trade Area of the Americas conference.[31]

In Canada, CCLA observes that the federal police force (RCMP) first confirmed their IMSI catcher use at the national level on 5 April 2017 (a use that was long suspected).[32] Other policing services have also been found to use them (e.g. Toronto Police Service).

In Ireland, Irish Council for Civil Liberties (ICCL) and INCLO described in INCLO's 2015 *Surveillance and Democracy* report[33] strong evidence suggesting that An Garda Síochána (the Irish police service) may have used stingrays to spy on the Garda Síochána Ombudsman Commission. Subsequently, Digital Rights Ireland and Privacy International made 2015 UN submissions on IMSI catchers in Ireland, describing this problem and arguing for criminalisation of IMSI catcher use.[34]

In South Africa, the Legal Resources Centre (LRC) describes media reports with on and off-record comments by police sources strongly suggesting that government agencies have bought and used IMSI technology themselves, potentially against student protesters in the #feesmustfall movement.[35]

In the United Kingdom, Liberty has been fighting alongside Privacy International to unearth police use of IMSI catchers, noting tools are particularly ripe for abuse when used at public gatherings, such as protests, where the government can easily collect data about all those attending.[36]

Pineapples

First released in 2008 by Hak5, Pineapples allow easily executable attacks on public Wi-Fi networks.[37] They use multiple radios and can therefore interface

[31] Available at: http://cdn.arstechnica.net/wp-content/uploads/2013/09/miami-dade.pdf
[32] Dave Seglins et al, 'RCMP reveals use of secretive cellphone surveillance technology for the first time' (*CBC News*, 5 April 2017) available at: https://www.cbc.ca/news/technology/rcmp-surveillance-imsi-catcher-mdi-stingray-cellphone-1.4056750
[33] Available at: https://www.inclo.net/pdf/surveillance-and-democracy.pdf
[34] See Privacy International and Digital Rights Ireland, 'The Right to Privacy in Ireland' (September 2015), paras. 54-56: https://privacyinternational.org/sites/default/files/2017-12/upr_ireland.pdf
[35] Further evidence of police use of 'grabbers' was detailed in an investigative report in the *Mail & Guardian* newspaper.
[36] Liberty, 'Privacy International and Liberty fight to unearth police use of intrusive mobile phone monitoring technology' (7 August 2018) available at: https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/privacy-international-and-liberty-fight-unearth-police-use
[37] Daniel Oberhaus, 'How a Wi-Fi Pineapple Can Steal Your Data (And How to Protect Yourself From It)' (*Motherboard*, 20 November 2017) available at: https://motherboard.vice.com/en_us/article/pa39xv/pineapple-wifi-how-to-mitm-hack

with hundreds of devices at a time, and are optimised to execute complicated network attacks.

> **In Colombia, Dejusticia** describes how the Inspector General's Office has already conducted the first part of an investigation into misuse, lying and corruption in the public forces and is moving forward on investigating the alleged purchase of Wi-Fi Pineapples.[38] The intelligence services in Colombia have a track record of spying and monitoring political opponents, social leaders and human rights movements.[39]

1.4 Internet bans

While not an example of online surveillance technology, internet bans can preclude the ability to protest or organise online. A person can be banned by law from publishing protest comments online. Technically, the bandwidth required to communicate can be throttled during times of protest, slowing or halting internet access and service.

> **In India** statistics show how internet shutdowns have almost become part of the standard operating procedures of the state during times of perceived unrest. The longest internet shutdown was 133 days in 2016 and there was another long shutdown of 100 days in 2017.[40]

> **In South Africa** and neighbouring countries, media reports indicate that government-directed internet outages have become the rule rather than the exception. Several countries, such as Gabon, Ethiopia, Chad, Uganda, Zimbabwe and South Africa, have shown in recent years that they are willing and capable of shutting down the internet or blocking mobile signals to stifle unfavourable content.[41]

---

[38] Bulletin 392 of the Inspector General's Press Office, available in Spanish at: https://www.procuraduria.gov.co/portal/juicio-disciplinario-a-general-y-oficiales-de-inteligencia-gastos-reservados.news. For more information about this investigation, see Bulletin 191 on the disciplinary investigation into the use of reserved expenditures, available in Spanish at: https://www.procuraduria.gov.co/portal/Gastos-reservados_-procuraduria-pide-suspender-pagos-e-indaga-seguimientos.news

[39] Dejusticia, 'Access to intelligence and counterintelligence archives in the framework of the post-agreement' (16 March 2017) available at: https://www.dejusticia.org/en/publication/access-to-intelligence-and-counterintelligence-archives-in-the-framework-of-the-post-agreement/

[40] Track shutdowns at: https://www.internetshutdowns.in

[41] Abdi Latif Dahir, 'More African governments blocked the internet to silence dissent in 2016' (Quartz Africa, 31 December 2016) available at: https://qz.com/africa/875729/how-african-governments-blocked-the-internet-to-silence-dissent-in-2016/. See also James Thompson, 'How Zimbabweans stayed online when government shut down the internet' (*TimesLIVE*, 18 January 2019): https://www.timeslive.co.za/news/africa/2019-01-18-how-zimbabweans-stayed-online-when-government-shut-down-the-internet/

Part 2. Rights impacted and INCLO criteria

2.1 Rights impacted

Our INCLO member case studies demonstrate the increasing use of online surveillance technologies by policing institutions in protest contexts. These case studies show real harms for democratic norms from these expanding powers: harms to individuals and their civil and human rights; harms to public trust and to the climate for political activism and dissent; and harms to the rule of law and the very fabric and structures of democratic societies. Protesters are being harassed, intimidated, scared away and barred outright from exercising their enshrined protest rights through the application of these technologies.

The fact that these powerful online surveillance technologies tend to be deployed by policing institutions in secret undermines policing based on openness, transparency and trust and deteriorates the relationship between policing institutions and the public. Massive collection and retention of personal information facilitated by online surveillance technologies treats everyone in, or in the vicinity of, a protest or a protest group as a suspect. It is by definition not justified by any individualised determination, and it violates the principles of legality, necessity and proportionality.

This scenario under which surveillance technologies are used is compounded by an increasingly adverse climate towards democratic dissent and civic space. Ever more frequently, governments are adopting policies to regulate and restrict the rights to protest by establishing authorisation and notification systems, arming their policing institutions with often unregulated crowd-control weapons and granting them discretionary powers to repress and disperse protests, while also detaining leaders of protests and social movements and resorting to unlawful use of force. These measures show a growing intolerance towards dissent and the expression of grievances and claims and indicate that state and policing institutions tend to identify protests, assemblies and other gatherings as security threats. This therefore raises the question of why and for what purposes these surveillance technologies are being used. If their use is premised on the notion that a protest is a security threat, this use is illegal. The rights to protest

and assembly have long been protected by international law principles and standards, as well as by most national constitutions and domestic laws.[42]

The normative framework outlined here requires an understanding on the part of the state and its policing and security institutions about their role and the role of protests in a democratic society.

Specifically, it requires an understanding that protests – however small or large, however critical of the establishment or disorderly they may be – represent an exercise of essential democratic rights that are protected under international law. However, a look at the policing models dominant over the last century reveals a different understanding – one of hostility towards protests with a focus on dispersing crowds and stifling dissent. Additionally, there is a legacy relating to the historical use of intelligence practices, including surveillance technologies, that cannot be disregarded especially against historically marginalized and discriminated communities. Intelligence gathering and surveillance tactics have been used by policing institutions as tools of political and ideological persecution with the goal of silencing dissent, disrupting people's ability to organise, cracking down on social movements, and delegitimising their leaders and their social demands.

It is in this context that the question of why and for what purposes online surveillance technologies are being used regarding protest becomes ever more relevant. Other reasons exposed by the state are the need to use these technologies to prevent clashes between different groups in the context of a protest, or to investigate a crime which might coincide with a protest or have suspects involved in a protest. In either of these two scenarios, the use of this surveillance still raises many questions and is still done without following proper judicial procedures and under very opaque circumstances.

2.2 Need for international standards

There are few international standards with clear guidelines to direct states as to how online surveillance technologies might be used by policing institutions in the

[42] Under the International Covenant on Civil and Political Rights (ICCPR), the realisation of the right to assemble and to protest requires the protection of a broad range of fundamental human rights, including the rights to: life; liberty and security of person; humane treatment and respect for the inherent dignity of the person; the right to privacy; the right to hold opinions, and freedom of expression; the freedom to associate with others; the right to non-discrimination in the enjoyment of each of these rights; and the right to an effective remedy in the case of the violation of human rights. As we note in *Defending Dissent* (p. 6): 'Collectively, these rights comprise "the rights to protest", the core rights a state must protect and promote to enable the exercise of protest and public assembly.' As acknowledged in the words of the Special Representative of the UN Secretary-General on human rights defenders: 'The protection of the right to protest lies in the recognition and protection of a set of rights that includes freedom of expression and opinion, freedom of association, freedom of peaceful assembly and trade union rights, including the right to strike' (*Report of the Special Representative of the Secretary-General on human rights defenders*, UN Doc. A/62/225 of 13 August 2007, para. 12.).

context of protests.[43] Important considerations include how these technologies should be prohibited or regulated, what protections and safeguards should exist, how abuses should be investigated and perpetrators be held accountable, and what kind of mechanisms for control, oversight and accountability should be developed. **Further, the cumulative effect of these technologies on human rights has yet to be evaluated, and as such the international community has not properly considered the question of whether it should *ever* be permissible to deploy some or all of these technologies, in protest contexts or at all.**

2.3 INCLO criteria for recommendations

Prefaced by our concern about whether use should ever be permissible, INCLO proposes here criteria intended to guide international standards regarding online surveillance technology, taking into account that specific human rights are at stake when they are used in relation to protests.

Negative impacts of online surveillance on fundamental rights in protest contexts

At the outset we recommend that the use of indiscriminate online surveillance technologies by policing institutions should be prohibited. Further, any legislation or action that prohibits protest online or provides unrestricted access to personal data by policing institutions via surveillance technologies is contrary to the right to protest.

Objective evidence

Objective evidence connecting the need for online surveillance technologies to the protesting subject being surveilled should be mandatory in all cases.

[43] It is worth noting that as a starting point, various bodies have expressed that limits must be placed on the use of these technologies. The previous UN Special Rapporteur joint report stated explicitly that '[t]he collection of personal information in relation to an assembly must not interfere impermissibly with privacy or other rights' and must be regulated by national law that complies with human rights: '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', UN Doc. A/HRC/31/66 (4 February 2016), para. 5. Similarly, the African Commission on Human and Peoples' Rights (ACHPR) Guidelines state that any 'documenting of assembly operations by law enforcement officials must be regulated by national law in compliance with regional and international human rights standards' and also that recording and surveillance cannot be used 'as a means to harass or intimidate assembly participants, or to discourage persons or groups from exercising their right to assemble freely with others.': ACHPR, 'Guidelines for the Policing of Assemblies by Law Enforcement Officials in Africa', paras. 15.2-15.3 The ACHPR Guidelines also state that any 'retention and use [of information] should be limited to circumstances where the use of force by law enforcement officials or their exercise of the powers of arrest and detention is recorded; where a complaint about the conduct of law enforcement officials is made; where recordings provide evidence of misconduct by law enforcement officials; or where recordings provide evidence of a crime committed by law enforcement officials or others. Recordings should be retained only for so long as is necessary for the relevant purpose.' See paras. 15.2-15.3.

Authorisation must rely on objective evidence and come from a judge or similar independent body **in all cases**.

Targeted surveillance

The use of targeted as opposed to general surveillance by policing institutions utilizing online surveillance technologies should be mandatory.

Strict necessity

In the case when there is an allegation of a suspected serious criminal offences[44] or risks to public security,[45] limit policing institutions' collection of personal data by online surveillance technologies to that which is strictly necessary. The indiscriminate collection of any personal data should be prohibited. The data collected must be precisely categorised to preclude the collection of irrelevant content. Any information that is categorised as irrelevant should be deleted and the deletion documented.

Data distribution

Data collected by policing institutions via surveillance technologies must not be distributed to other government agencies unless the person is in some way implicated in a serious crime.[46] The transferred data must also relate strictly to the investigation, prosecution or prevention of that serious crime. Policing institutions must not share or retain any material that is not relevant to the investigation at hand. As INCLO describes in our *Unanswered Questions* report on intelligence sharing,[47] there is a general lack of public information about the normative framework regarding the exchange of this kind of information between countries. There are also clear regulatory gaps. We provide high level recommendations on this specific problem in *Call for action – Regulate Intelligence Sharing*, including guidance for governments, intelligence agencies, and independent oversight bodies.[48]

---

[44] Our use of the terms 'serious criminal offences' or 'serious crime' also acknowledges that these terms require rigorous standards that are compatible with human rights protections. We look, as an initial point of exploration, to the articulated legal standard in Article 2, subparagraph (b), of the Organized Crime Convention: 'conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty' see: https://www.unodc.org/documents/treaties/organized_crime/COP6/CTOC_COP_2012_CRP/CTOC_COP_2012_CRP4.pdf. However, we acknowledge also that this standard **can still lead to abuses of human rights** for example in instances where legislation prohibits protest altogether and/or is accompanied by lengthy terms of liberty deprivation.

[45] Similar to our point at footnote 44 about defining serious crime, 'public security' should be clearly defined in the regulatory frameworks before arguments of 'safeguarding public security' are deployed, lest they be used as a pretext for massive/systematic surveillance or undue interferences with human rights.

[46] See again our qualification of this term at footnote 44.

[47] Available at: https://www.inclo.net/pdf/iisp/unanswered_questions.pdf

[48] 2018 with Privacy International - https://www.inclo.net/pdf/Intelligence-Sharing-Brochure-WEB.pdf

Notification

Those protesters whose personal data is collected via online surveillance technologies deployed by policing institutions must be notified as soon as notification is not likely liable to jeopardise the legitimate investigations undertaken - targeted surveillance must not relate to protest per se, but with the criminal facts that are under investigation. Notification should include full disclosure of the procedure that led to online surveillance and of the information that was gathered through it.

Awards and judicial remedies

Compensation must be awarded to protesters whose personal data has been collected and accessed in contravention of their rights. Legislation should also expressly provide for an appropriate judicial remedy (i.e. judicial review) and associated procedures for when policing institutions' use of online surveillance technology breaches protest rights.

Transparency

Policing institutions should be monitored and required to account for their activities. They should report to independent oversight bodies with statistics about who they deployed surveillance technologies against, the types of surveillance technologies deployed, which precisely categorised sets of data were collected, the circumstances of strict necessity involved, third party distribution, and awards or judicial remedies issued.

Oversight

Strong oversight mechanisms for policing institutions and their use of surveillance technology are required, in order to ensure accountability and redress when these surveillance tools are misused. Independent and sufficiently resourced offices with the technical expertise to understand the surveillance technologies being deployed are key. Public transparency reports and regular parliamentary engagement should be part of the oversight mechanism mandate.

Social media networks

- Using social media and other online mechanisms to invite people to participate in a protest is protected by the right to participate in protests.[49] Legislation that permits unrestricted access to social media by policing institutions is contrary to protest rights.
- Policing institutions may not conduct mass surveillance via unrestricted access to social media accounts – open or closed. As with offline

[49] See Opinion No. 6/2016 adopted by the UN Working Group on Arbitrary Detention (6 June 2016): https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session75/Opinion_2016_6_Egypt.pdf

investigations, police must first seek judicial authorisation on a case-by-case basis.

- Judicial authorisation may not permit policing institution access to social media accounts writ large. Courts must limit the range of data sought, limit access only to material that is relevant to criminal investigations or prosecutions, and require that third party information, including photos, names and comments, be edited out entirely.
- Policing institutions should not share or retain any material it cannot prove relevant to the investigation at hand.
- Similarly, policing institutions may only retain this social media information for a limited period of review.
- A neutral oversight body or at minimum a court-approved search protocol could be used to review material in order to ensure policing institutions do not receive information that is irrelevant to their search.
- The account holders whose accounts are in question must be notified of the search, in non-urgent cases in advance, so they have the opportunity to seek court intervention.

Recording, face surveillance and protester databases

- A generalised and undefined belief that someone taking part in a protest may commit some offence in the future is an example of offensive and baseless profiling that does not justify surveilling, taking or retaining a photograph, or recording video footage of protesters. Any recording of a protest by policing institutions should be open, transparent, publicised and for the purpose of protecting the protest and the protesters, with the goal of using the material for review and evaluation of police intervention in the protest.
- Policing institutions should cease to use face surveillance in public spaces.
- States should not collect or store any personal information on databases. A clear protocol about how to select, save, store, preserve, access and delete personal data should be in place for temporary data collections, along with mechanisms and processes to promote public access to the recordings – particularly in cases where force is used.

Hacking

- Policing institutions' use of IMSI catchers in protest contexts should cease, **especially** in jurisdictions where authorities are not following international standards or there are no robust safeguards in places.

Internet bans

- INCLO observes that any legislation or action that prohibits protest online in the form of internet bans is contrary to our protest rights. We concur with the UN Human Rights Council's affirmation in a resolution approved during its 32nd session that 'the same rights people have offline must also be protected online', and we share its deep concern at 'measures aiming to or that intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law.'[50] Our rights to protest and associate rights require unfettered access to the internet, and limitations or restrictions on access should be illegal in all circumstances for precluding those rights.

[50] See UN Doc. A/HRC/32/L.20 on the promotion, protection and enjoyment of human rights on the Internet (27 June 2016): https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Part 3. Case studies in our 13 INCLO member countries

3.1 Agora - Watching protesters online is state policy in Russia

Damir Gainutdinov, Legal Analyst

In Russia, policing institutions deliberately scan social media networks for protest activity. Police register accounts on social media networks, join various protest groups and even friend civic activists in order to watch and document online posts.[51]

As a rule, the police also collect evidence of online protest activity from social media networks in order to build administrative and criminal cases against activists. Screenshots from social networks have become staple building blocks of the body of evidence.

Russian policing institutions have also organised an information exchange with most of the social media companies operating in the country and under Russian jurisdiction. As a result, the police can obtain IP addresses without difficulty. They use these to subsequently identify the users' details, such as telephone numbers, residential addresses and other personal information.

Policing institutions also use this gathered information to build databases on protesters and activists and to add them to a preventive watchlist as opposition-minded citizens. This data subsequently surfaces in various unrelated public documents. In building their database, the police are also helped by general citizen databases, such as the TOR Software Complex, used in Tatarstan. This records all instances in which a citizen has interacted with the police, as well as data on that person's movements using all modes of transport (airplane, train, bus).

Examples of the negative effects of this online surveillance include the experience of Aleksandr Valov of Sochi, who was subject to operative investigative activities by reason of 'involvement with a group of opposition-minded citizens'.[52] Another example lies in the administrative case brought against Dmitry Teterin, which contained a report from the Centre for Combating Extremism stating that he was a 'member of the anti-establishment opposition and is engaged in fomenting

[51] See for example the courtroom testimony of this police agent who 'friended' a group of activists and was included by them in their mailing list (*MediaZona*). Available in Russian at: https://zona.media/chronicle/delo_sokolova#9597

[52] Natalya Kondrashova, 'Commitment to opposition views justifies surveillance' (*RFE/RL*, 12 August 2018) available in Russian at: https://www.svoboda.org/a/29428501.html

protest moods among the residents of the city'.[53] Teterin's experience is also an example of how those previously found liable for so-called extremist offences can then be cautioned by the prosecutor's office about engaging in protests that might also be interpreted by the state as extremist.[54]

Finally, Russian policing institutions are also known to use SORM system technology to trace people's locations. This technology enables policing institutions to approach mobile operators and request a customer's billing information. Indirect indications that such data has been used for the covert surveillance of protesters and activists have come to light repeatedly. The police often locate activists in the places the activists frequent (cinemas, country houses, cafés), even when these citizens have not revealed their whereabouts. For example, on 20 January 2019, a public prosecutor came to an informal meeting of 'Open Russia' activists at the city café in Cheboksary and handed a subpoena to Yuriy Sidorov.[55]

3.2 ACLU - Fighting US Facebook search warrants against protesters[56]

Washington-DC office

The ACLU of the District of Columbia went to court to block the enforcement of search warrants targeting three Facebook accounts as part of the government's investigation and prosecution of activists arrested on Inauguration Day 2017 in Washington DC.

Two of the warrants would have required Facebook to disclose to the government all information from the personal Facebook profiles of local DisruptJ20 activists Lacy MacAuley and Legba Carrefour from 1 November 2016 through 9 February 2017. Although the warrants claimed to only seek evidence in support of government prosecutions related to Inauguration Day demonstrations on 20 January, they demanded – among other things – all private messages, friend lists, status updates, comments, photos, videos and other private information solely intended for the users' Facebook friends and family, even if they had nothing to do with Inauguration Day. The warrants also sought information about actions taken on Facebook, including all searches performed

[53] Regina Gimalova, 'The court sentenced an activist from Tatarstan to a fine' (*Idel.Real.,* 28 August 2018) available in Russian at: https://www.idelreal.org/a/29457768.html
[54] Vadim Mescheryakov, 'WTOA activist tried to declare illegal the warning of the prosecutor's office about the inadmissibility of extremist activity' (*Idel.Real.,* 13 December 2017) available in Russian at: https://www.idelreal.org/a/28913769.html
[55] Yuriy Sidorov, personal Facebook account (20 January 2019), available in Russian at: https://m.facebook.com/story.php?story_fbid=2263701970584620&id=100008345174557
[56] See also ACLU, 'ACLU-DC seeks protection for personal Facebook accounts against Inauguration Day search warrants' (28 September 2017): https://www.aclu.org/news/aclu-dc-seeks-protection-personal-facebook-accounts-against-inauguration-day-search-warrants-0

by the users, the groups or networks they joined, and all 'data and information that has been deleted by the user'.

The third search warrant was issued for the DisruptJ20 Facebook page (now called 'Resist This'), administered and moderated by Emmelia Talarico. Although the page is public, the warrant would have required the disclosure of non-public lists of people who planned to attend political organising events and even the names of people who simply liked, followed, reacted to, commented on or otherwise engaged with the content on this Facebook page. During the three-month span covered by the search warrant, approximately 6,000 Facebook users liked the page.

The warrants were overbroad and in violation of the Fourth Amendment (which protects personal privacy) and were particularly problematic because they sought to reveal the lawful political associations and activities of the users and of thousands of third parties. Opening up the entire contents of a personal Facebook page would allow the government to reach deeply into individuals' private lives. Governmental agents would discover a detailed portrait of individuals' protected political activities and associations.

When policing institutions can comb through records concerning political organising in opposition to the very administration for which their officers work, the result is the chilling of First Amendment-protected political activity. Ultimately, in July 2018, the government dropped the last of the criminal charges against protesters for their Inauguration Day conduct; accordingly, the warrants the ACLU had challenged became moot.[57]

This is one of other known attempts by the US government to conduct unlawful dragnet searches of the internet and social media in order to seek evidence against the protesters arrested on Inauguration Day. In a similar case of state overreach, the government had issued a warrant to website hosting provider

[57] Keith L. Alexander, 'Federal Prosecutors Abruptly Dismiss All 39 Remaining Inauguration Day Rioting Cases,' *Washington Post*, July 7, 2018, available at: https://www.washingtonpost.com/local/public-safety/federal-prosecutors-abruptly-dismiss-all-remaining-inauguration-day-rioting-cases/2018/07/06/d7055ffe-7ee8-11e8-bb6b-c1cb691f1402_story.html?noredirect=on&utm_term=.df307ed8281c. See also ACLU, 'In the Matter of the Search of Information Associated with Facebook Accounts disruptj20,' available at: https://www.acludc.org/en/cases/matter-search-information-associated-facebook-accounts-disruptj20-etc.

Dreamhost for the IP addresses of the 1.3 million people who ever visited the DisruptJ20.org website.[58]

3.3 ACRI – Detention of student over Facebook BDS activity

Avner Pinchuk, Unit Director and Chief Operating Officer, Civil and Political Rights Unit

In March 2017, the Knesset passed a law banning the entry of supporters of the Boycott, Divestment and Sanctions (BDS) movement against Israel. The Immigration Authority and the Ministry for Strategic Affairs can prevent the entry of anyone suspected of supporting BDS on the basis of information gathered on internet sites and social media.

Lara Alqasem, a 22 year old American student, landed at Ben Gurion Airport on 2 October 2018 for Master's degree studies at Jerusalem's Hebrew University.[59] Despite having a visa, she was denied entry. Alqasem, reportedly of Palestinian descent, had been the president of a local chapter of the pro-boycott Students for Justice in Palestine (SJP) group while she was a student at the University of Florida. The state alleged that she continued to support the movement to boycott Israel. Alqasem insisted she had left the SJP in 2017 and was not active in any boycott group. She decided to challenge the decision in court, and she stayed at the airport detention facility for 15 days until the Supreme Court approved her appeal.

The ministry uses a variety of sources to identify BDS activists, including tips from informants and social media posts. The ministry says its suspicions were deepened after learning that Alqasem recently deleted all of her social media accounts.[60] The Hebrew University, which backed Alqasem in court, has slammed the state for allegedly sloppy and superficial Facebook-style evidence versus testimony from Alqasem's University of Florida professors who know her.[61]

The Tel Aviv Magistrate's and District Courts dismissed Alqasem's appeal, saying she was still a 'potential risk', but the Supreme Court overturned her

[58] In the Matter of the Search of www.disruptj20.org That Is Stored at Premises Owned, Maintained, Controlled, or Operated by Dreamhost, Spec. Proc. No. 17 CSW 3438, slip op. at 6-7 (D.C. Super. Ct. Oct. 10, 2017)
[59] *The Times of Israel*, 'Hebrew U. head backs detained US student, warns case harms anti-BDS efforts' (9 October 2018) available at: https://www.timesofisrael.com/hebrew-u-head-backs-detained-us-student-warns-case-harms-anti-bds-efforts/
[60] *The Times of Israel*, 'Hebrew U. head backs detained US student, warns case harms anti-BDS efforts' (9 October 2018) available at: https://www.timesofisrael.com/hebrew-u-head-backs-detained-us-student-warns-case-harms-anti-bds-efforts/
[61] Josh Axelrod, 'Hebrew University protesters reserve empty chair for alleged BDS activist' (Jerusalem Post, 15 October 2018) available at: https://www.jpost.com/BDS-THREAT/Hebrew-University-reserves-empty-chair-for-alleged-BDS-activist-Alqasem-569437

deportation.[62] The three judges questioned the factual basis for the decision to deport Alqasem, and how refusing her entry helped the fight against boycotts and met the law's criteria, given the testimonies of the Hebrew University and others who supported her claims.

However, the court ultimately ruled in Lara Alqasem's favour, stating that her actions did not sufficiently warrant banning her entry to Israel, and that therefore 'the unavoidable impression is that her political opinions were the reason behind the cancellation of the visa that was granted to her', adding 'if that is indeed the case, we are talking about a radical and dangerous step.'[63]

Not discussed in detail by the court was the chilling effect such overt surveillance of protest activities on social media by the Israeli state might have on those seeking to rally against persecution.

ACRI - Facebook prevents ACRI from publishing protest ads[64]

Tel Aviv

Sometimes social media companies themselves quell protest activities. In June 2018, ACRI's English Facebook[65] ads regarding incidents of racism in Israel were not approved by Facebook. Facebook gave the following explanation to ACRI: 'Your ad was not approved because your Page has not been authorised to run ads with political content.'

This corporate policing of online protest is part of Facebook's new policy that no longer permits promoting ads that Facebook has defined as containing 'political content' – unless the Facebook page owner is a registered US citizen. As a result of attempting to share posts protesting against the new 'nation-state law' in Israel[66], ACRI has de facto been blocked from promoting any content on its English Facebook page.

---

[62] Josh Axelrod, 'Hebrew University protesters reserve empty chair for alleged BDS activist' (Jerusalem Post, 15 October 2018) available at: https://www.jpost.com/BDS-THREAT/Hebrew-University-reserves-empty-chair-for-alleged-BDS-activist-Alqasem-569437

[63] *The Times of Israel*, 'A "big victory for BDS": Ministers pan Supreme Court for letting student stay' (18 October 2018) available at: https://www.timesofisrael.com/a-big-victory-for-bds-minister-pans-supreme-court-for-letting-student-stay/

[64] ACRI notes that this case is an exception to the focus on governmental interference in these submissions. They comment however that the role of private social media companies might be included in our definition of 'policing institutions.' This is because their use of online technologies to limit protest can have a powerful impact; they might therefore be included in that club of powerful institutions.

[65] See: https://www.facebook.com/acri.eng/

[66] These are the relevant posts, which both protest the new 'nation-state law' in Israel: https://www.facebook.com/acri.eng/photos/a.175582895812431.30348.175570835813637/1729813257056046/?type=3&theater; and https://www.facebook.com/acri.eng/photos/a.175582895812431.30348.175570835813637/1729339293770109/?type=3&theater

3.4 CCLA - Filming student protests in Canada

Rob De Luca, Director, Democracy and the Rule of Law Program

In 2018, numerous protests took place at York University, one of the largest universities in Canada. The protests were in support of a strike by a local union representing almost 2,000 education workers at the university. The protests included peaceful 'sit-ins' on university premises by both non-union students and unionised education workers. Online videos arising from the protest and competing online communications became a staple of the negotiations.[67] The strike began on 5 March 2018 and ended in July 2018 via government back-to-work legislation.

The university's policing of these protests raised troubling concerns regarding the use of surveillance techniques to chill and sanction protest participants. In direct response to the strike action, the university hired private security officers to supplement its campus police force. Protesters were then regularly filmed throughout the strike via surveillance cameras.[68] As one student, Karmah Dudin, noted, '[s]ecurity members were present – some in plain clothes – at any protest or gathering, recording us. No one knew where these pictures and videos would be stored or for what purposes they would be stored.'[69] The university administration also regularly cited protesters' social media communications (such as communications that made disparaging remarks regarding key university administrators) in publicly available letters and communications, routinely posted online, that were disparaging of protester conduct.[70]

In an informal poll conducted by the Canadian Civil Liberties Association (CCLA), 68% of respondents (132 out of 194 in total) stated that they were filmed without their consent.[71] An additional 68% (131 out of 192 respondents) stated that they felt they were being surveilled and were having information collected about them. Some individuals separately expressed concern that this surveillance may have extended to the university email accounts of education workers and/or students. Forty per cent of respondents (76 out of 190) stated that the university's surveillance of protest activities discouraged them from taking part in the protests.

---

[67] See for example Canadian Union of Public Employees, 'CUPE 3903 Condemns the Use of Violence to Repress Dissent on Campus' (25 March 2018) available at: https://3903.cupe.ca/2018/03/25/cupe-3903-condemns-the-use-of-violence-to-repress-dissent-on-campus/

[68] A.T. Kingsmith, 'Strike Surveillance' (*Briarpatch Magazine*, 29 October 2018) available at: https://briarpatchmagazine.com/articles/view/strike-surveillance

[69] A.T. Kingsmith, 'Strike Surveillance' (*Briarpatch Magazine*, 29 October 2018) available at: https://briarpatchmagazine.com/articles/view/strike-surveillance

[70] See for example 'York's Response To CUPE 3903's Letter – April 11, 2018' available at: https://labour.yorku.ca/2018/04/12/york-university-responds-to-letter-from-cupe-3903/

[71] CCLA, 'Preliminary Report on Rights Violations at York U - Survey Results' (29 March 2018) available at: https://ccla.org/yorku-strike-survey-results/

While the full impact and extent of the surveillance that was used during the York University strike is difficult to determine, the above poll results indicate how the ever-increasing use of video recordings as a surveillance tool, in conjunction with social media surveillance, can chill rights to protest. The incident highlights how individuals can oftentimes be deterred by 'offline' surveillance techniques because of their appreciation of how pictures, videos and other information can be digitally stored and shared online.

The case also highlights concerns that certain activists may be targeted for reprisal due to their active presence on social media and for other journalistic activity, both traditional and non-traditional, during protests. For instance, student Karmah Dudin stated she has received several threats of reprisal from York security, and that her status as a 'known dissenter' resulted in a 'precarious' position as regards her student and employment status at the university.[72] Despite the substantial number of students involved in the protests, the university has pursued administrative proceedings against just eight individuals, with several of those students claiming that they were among the few individuals targeted for discipline because they were active on or collaborated with media.[73]

3.5 CELS - Watching activists online in Argentina

CELS

In December 2017, two people arriving in Buenos Aires as intended civil society representatives at the WTO's 11th Ministerial Conference were deported. They were among 65 people from civil society organisations throughout the world whose WTO-approved accreditation had been rejected by Argentine security authorities 'for unspecified reasons'.[74]

In response to the controversy that arose, a Foreign Affairs Ministry press release justified the decision to reject the accreditations on the grounds that the organisations or their members 'had made explicit calls via social media for violent demonstrations, expressing their intent to generate intimidation and chaos.'[75] Clearly, the Argentine government had been gathering intelligence, very possibly based on people's organisational affiliation or political opinion – which is expressly prohibited under Argentine law.[76]

---

[72] A.T. Kingsmith, 'Strike Surveillance' (*Briarpatch Magazine*, 29 October 2018) available at: https://briarpatchmagazine.com/articles/view/strike-surveillance

[73] *CityNews* (video), 'Students facing possible discipline after York strike protest' (7 September 2018) available at: https://toronto.citynews.ca/video/2018/09/07/students-facing-possible-discipline-after-york-strike-protest/; see also Victoria Silman, 'The Fate of Eight' (*Excalibur*, 20 September 2018): https://excal.on.ca/the-fate-of-eight/

[74] The government presented the list of 65 people whose accreditations were rejected at a court hearing on 9 December.

[75] Press release available at: https://cancilleria.gob.ar/es/actualidad/comunicados/sobre-la-acreditacion-de-ongs-la-conferencia-ministerial-de-la-omc-en-buenos

[76] National Intelligence Law 25.520, as modified by Law 27.126

The two people who were ultimately deported – Petter Titland from Norway and British-Ecuadorean journalist Sally Burch – decided to travel to Argentina despite having their accreditations rejected, to participate in other activities. When Titland arrived, he was detained for about ten hours in the Ezeiza International Airport. Immigration officials accused him of being a 'false tourist' and deported him to Brazil in the early morning hours of the next day. Burch was also deported.

At a court hearing on the habeas corpus filed on behalf of the activists, the government presented the list of 65 people whose accreditations had been rejected, but insisted that the list did not impede entry to Argentina and had no bearing on the deportation of Titland or Burch. It did acknowledge, however, that the Foreign Affairs Ministry sent this list to the National Migrations Office, as an 'alert'. Both Titland and Burch's names appeared there.

Thanks to legal[77], diplomatic and media pressure, no one else was prohibited from entering the country. The Argentine government also announced it was reaccrediting some of the people on the list of 65, including Petter Titland. However, many other individuals and organisations remained without accreditation, including Chilean NGO Derechos Digitales, Argentine NGO Fundación Grupo Efecto Positivo and British NGO Global Justice Now.

The chilling effects of this surveillance and vetting process are clear. Some activists who were disaccredited by the state chose not to travel to Argentina out of fear. Others had their visas rejected. Some continue to worry that these marks will stay on their migration record. These actions by the Argentine government sent a disturbing message regarding the country's commitment to civil society participation.

Less clear are the exact surveillance mechanisms employed to disaccredit would-be participants based on their social media use. CELS has filed administrative petitions for access to information on the process of vetting attendees. The results have not shed much light. The Federal Intelligence Agency (AFI), for example, responded that this information is necessarily secret for national security reasons, despite the fact that CELS is requesting personal information.

In general, the process to access public or personal information regarding security issues is very difficult and opaque, and even 'National Security' is usually invoked as a generic answer for rejection to provide information. Both the administrative and judicial procedures are inefficient, and there is no intention to control what information is being produced and gathered by intelligence bodies,

[77] CELS intervened in this conflict prior to the deportations, filing legal and administrative petitions and collective habeas corpuses as soon as we learned that activists whose accreditations had been rejected were being retained at the Ezeiza airport (most of these people were eventually allowed to enter the country, but only after their embassies intervened). During the 9 December hearing, CELS' lawyers obtained assurances from the National Migrations Office that none of the people on the list had been banned from entering the country, including Titland and Burch.

or who is being spied on and under what criteria, to determine whether those activities are legal or not.

3.6 Dejusticia - Suspected use of Wi-Fi Pineapples in Colombia

Vivian Newman Pont, Director; Santiago Virgüez, Researcher; and María Paula Angel, Researcher

In Colombia, there is no information about the use of IMSI catchers. However, a technology known as Wi-Fi Pineapples has been mentioned in the press. A Wi-Fi Pineapple is a piece of hardware that was originally created for network penetration testing. Penetration testing is an authorised attack of a system in order to find vulnerabilities. According to an article in *Motherboard*:

> The Pineapple is a nifty little device first released in 2008 by Hak5, a company that develops tools for penetration testers, or 'pentesters.' Pentesters are usually hired by organizations to attack their own networks in order to expose vulnerabilities before they are discovered by some bad actors. The Pineapple allows pentesters to easily execute sophisticated attacks on public Wi-Fi networks to see how the attacks work and how to protect the network from those attacks. Pineapples aren't much different than the normal Wi-Fi access points you use to get internet at home or in the office, just more powerful. They use multiple radios rather than just a single radio found in most routers. This means a Pineapple is able to interface with hundreds of devices at a time, rather than just a few dozen. Moreover, the Pineapple's web interface is optimized to execute complicated network attacks.[78]

While originally developed to identify vulnerabilities, Pineapples can also be used to collect sensitive personal information from any and all users on public Wi-Fi networks, especially under two legal regulations that i) allow for 'monitoring' the electromagnetic spectrum without prior judicial authorisation;[79] and ii) conceive the electromagnetic spectrum (the space through which communications travel) as a public space where, therefore, there are no privacy rights.[80]

In Colombia, there is an ongoing disciplinary investigation by the Inspector General's Office against intelligence service officers – one general and two colonels – for irregularities in the use and control of reserved budgetary

[78] Daniel Oberhaus, 'How a Wi-Fi Pineapple Can Steal Your Data (And How to Protect Yourself From It)' (*Motherboard*, 20 November 2017) available at: https://motherboard.vice.com/en_us/article/pa39xv/pineapple-wifi-how-to-mitm-hack

[79] Article 17 of Law 1621 of 2013, available in Spanish at: http://www.secretariasenado.gov.co/senado/basedoc/ley_1621_2013.html#17

[80] Articles 32 and 139 of the Colombian National Police Code, available in Spanish at: http://www.secretariasenado.gov.co/senado/basedoc/ley_1801_2016_pr003.html#138

expenditures.[81] The inspector general has already conducted the first part of an investigation for misuse, lying and corruption in the public forces and is moving forward on investigating the alleged purchase of Wi-Fi Pineapples, which might have been used to intercept the communications of political and social leaders. The intelligence services in Colombia have a track record of conducting internal espionage and monitoring political opponents, social leaders and human rights movements.[82]

3.7 EIPR - Anti-protest law stifling online protest in Egypt

EIPR

The experience of Alaa AAbdel Fattah illustrates how anti-protest laws addressing physical space affect the ability of citizens to protest online. Alaa was arrested violently in 2013 after the government passed Law No. 107 effectively banning street protests.[83] He was accused of organising a gathering of more than five individuals that was likely to endanger public order, among other charges. A report from the Directorate of Information and Documentation showed that Alaa AAbdel Fattah used Twitter to ask people to demonstrate at the entrance to the Shura Council building, which was serving as the convening place for the Constituent Assembly.[84]

In addition to Twitter, the prosecution files and the court ruling in the case brought against Alaa and others also referred to Alaa's use of his personal page on Facebook (which, according to the court at the time, had 515,779 followers) to call for protesting against constitutional provisions that allow for the military trial of civilians. The court ruling made reference to two Facebook pages that copied Alaa's alleged call for protest and cited the fact that Alaa was a founding member of the group affiliated with one of the pages as the only evidence that he was responsible for the call to protest, in violation of the anti-protest law that had been enacted 48 hours before this particular demonstration.[85]

---

[81] Bulletin 392 of the Inspector General's Press Office, available in Spanish at: https://www.procuraduria.gov.co/portal/juicio-disciplinario-a-general-y-oficiales-de-inteligencia-gastos-reservados.news. For more information about this investigation, see Bulletin 191 on the disciplinary investigation into the use of reserved expenditures, available in Spanish at: https://www.procuraduria.gov.co/portal/Gastos-reservados_-procuraduria-pide-suspender-pagos-e-indaga-seguimientos.news

[82] Dejusticia, 'Access to intelligence and counterintelligence archives in the framework of the post-agreement' (16 March 2017) available at: https://www.dejusticia.org/en/publication/access-to-intelligence-and-counterintelligence-archives-in-the-framework-of-the-post-agreement/

[83] For more information, see Wafa Ben Hassine, 'The Crime of Speech: How Arab Governments Use the Law to Silence Expression Online': https://www.eff.org/files/2016/04/28/crime-of-speech.pdf

[84] See Opinion No. 6/2016 adopted by the UN Working Group on Arbitrary Detention (6 June 2016): https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session75/Opinion_2016_6_Egypt.pdf

[85] Case No. 12058/2013 Qasr el Nil Criminal Proceedings.

The UN Working Group on Arbitrary Detention, at its seventy-fifth session on 18-27 April 2016, adopted the opinion that Alaa AAbdel Fattah's use of Twitter to call on citizens to demonstrate did not offer evidence or prove that Alaa AAbdel Fattah was an organiser of the demonstration. Further, the working group considered 'that the use of Twitter for inviting people to participate in a peaceful protest is protected by the right of freedom of opinion and expression, as well as the right to disseminate ideas and participate in peaceful protests.' Its members opined that Law No. 107 seems contrary to international law, in particular to the right to freedom of peaceful demonstration.

Egypt's use of the anti-protest law to target activists is very widespread, with reach into the online sphere. Of parallel concern, EIPR's founder and former director, Hossam Bahgat, was previously arrested himself for publishing a report in an online newspaper investigating the criminal convictions of military personnel for plotting a coup. Egypt widely uses online activity and expression of opinion to criminally prosecute individuals.

3.8 India - Sentiment analysis of social media protests in India

Mumbai

In India, the state has broadened its mass surveillance project by focusing on 'sentiment analysis' and review of social media.[86]

The state already authorizes select security and intelligence agencies to watch, intercept, and decrypt any information generated, transmitted, received or stored in any computer resource.[87] Recent litigation at the Supreme Court, however, lead to the withdrawal[88] of the proposed Social Media Communications (monitoring) Hub. This was a proposal to 'collect digital media chatter from all core social media platforms as well as digital platforms... [i]n a single system providing real-time insights, metrics and other valuable data.'[89]

One of the key intentions behind the sentiment analysis programme is 'to track public views and sentiments on various social media platforms' in order to handle

[86] Amber Sinha of The Centre for Internet and Society, India, 'Social Media Monitoring', available at: https://cis-india.org/internet-governance/blog/social-media-monitoring
[87] Ministry of Home Affairs, Cyber and Information Security Division S.O. 6227(E) Order dated 20 December 2018, available at: http://egazette.nic.in/WriteReadData/2018/194066.pdf
[88] Kumar Sambhav Shrivastava, '40 government departments are using a social media surveillance tool – and little is known of it' (*Scroll.in*, 4 September 2018) available at: https://scroll.in/article/893015/40-government-departments-are-using-a-social-media-surveillance-tool-and-little-is-known-of-it
[89] Manas Tiwari, 'What is social media hub and how government plans to use it for monitoring WhatsApp messages, data' (*Financial Express*, 13 July 2018) available at: https://www.financialexpress.com/india-news/what-is-social-media-hub-and-how-government-plans-to-use-it-for-monitoring-whatsapp-messages-data/1243701/

'sensitive issues and protests.'[90] The technology, developed with state funding, provides for analysis of social media posts, categorising them as 'positive' or 'negative' and can create 'alerts' to authorities depending on the specific criteria they set out.[91]

With practically no oversight and a minimal response to citizen information requests, the state is moving ever closer to an Orwellian reality.

India - Internet bans during times of dissent in India

Delhi

Since 2012, internet shutdowns have practically become part of the state's standard operating procedures during times of perceived unrest. The longest shutdown was 133 days in 2016.[92]

Granting itself greater powers in 2017, the state created a set of broad rules authorising national or state-level officials to issue temporary suspension orders to shut down telecommunications services in times of public emergency or threats to public safety.[93]

In 2018, at least 134 incidents[94] of internet shutdowns were reported in which authorities ordered providers to restrict local mobile phone, SMS, wireless or occasionally fixed-line internet services[95]. A noticeable trend since last year is an increase in preventive shutdowns rather than responsive ones[96].

India has the highest number of incidents of internet shutdowns in the world and in the past few years the frequency, geographic distribution and length of shutdowns have all increased.[97] Public investigations are needed to study whether the shutdowns were executed through legal means. With broad powers on the state's side and limited checks and balances in place, the state seemingly uses shut downs against political discourse which it finds unpalatable on the one hand, but not against right-wing extremism on the other.

90 Amber Sinha of The Centre for Internet and Society, India, 'Social Media Monitoring', available at: https://cis-india.org/internet-governance/blog/social-media-monitoring
91 Amber Sinha of The Centre for Internet and Society, India, 'Social Media Monitoring', available at: https://cis-india.org/internet-governance/blog/social-media-monitoring
92 For more information see: https://www.internetshutdowns.in
93 Ministry of Communications, Department of Telecommunications G.S.R. 998(E) Notification dated 7 August 2017, available at: http://dot.gov.in/sites/default/files/Suspension%20Rules.pdf
94 For more information see: https://www.internetshutdowns.in
95 For more information see: https://www.internetshutdowns.in
96 For more information see https://www.internetshutdowns.in
97 For more information see: https://www.internetshutdowns.in

3.9 HCLU - Police creep social media for protest planning in Hungary

Szabolcs Hegyi, Expert, Political Freedoms Project

In Hungary, the police watch social media and online activity for protest event planning. This surveillance is the direct result of the new assembly law, passed in 2018, which introduces significant restrictions on the freedom of assembly. For example, the law requires protesters to notify the police about their plans for a gathering before they even make a call to protest. The effect of this law is that those organising protest events can no longer legally draw the attention of others to even tentative organising plans until after the police have examined them. This creates a practical obstacle: an organiser cannot anticipate how many people might participate, or the number of security measures required, without first making a call to action. It also creates a legal obstacle: violations of the procedural rules on notification constitute a minor offence, with accompanying monetary sanctions.[98]

The law is quite new, and so jurisprudence is still being developed. However, the HCLU is accumulating information on the reported police practice of watching social media. For example, the police sanctioned the local leader of a political party who did not notify them about a press conference regarding an anti-corruption campaign.[99]

The practical and legal consequences of this law for discussing, organising and publicising protests may dampen the use of social media and online discussion forums for these purposes. The law therefore has a potential chilling effect on organising protests and, more broadly, on civic activism. At the same time, it raises suspicions that the police watch social media in bad faith.

HCLU - Case study in Hungary of police filming protests

Szabolcs Hegyi, Expert, Political Freedoms Project

Filming protests in Hungary is now a regular practice, having become more pervasive after the riots and police brutality against protests in 2006.[100] Police are present at almost all assemblies or events drawing crowds, and they record from beginning to end. The police are legally permitted to record video and

[98] Fines can go up to 150,000 Hungarian forints (approximately 450 euros).
[99] More information available in Hungarian at: https://www.nyugat.hu/tartalom/cikk/momentum_szombathely_birsag_facebook_poszt
[100] The September 2006 riots came in response to Hungarian Prime Minister Ferenc Gyurcsany's admissions he had lied during the election campaign about the state of the economy so that he could remain in power (see: https://www.theguardian.com/world/2006/sep/19/1). A month later, as protests continued on the national holiday of October 23, even peaceful protesters became victims of police abuse and brutality (see: https://www.theguardian.com/world/2006/oct/23/1). For further details, see the HCLU's statements in Hungarian: https://tasz.hu/cikkek/a-tasz-sajtotajekoztatot-tartott-ma-a-2006-szeptemberi-es-oktober-23-ai-rendori-fellepes-tanulsagairol-video; and in English: https://hclu.hu/en/articles/invitation-to-hclu-press-conference-1

install CCTV cameras, but only if necessary for public safety or in the interest of preventing crimes.[101] Significantly, the police are also required to notify protest organisers that they will be doing this.

Both the original justification for the Police Act and the reasons behind its 2008 amendments were to safeguard protest rights, including the political and personal rights of the demonstrators, bystanders and journalists involved. By creating a record, it intended to prevent and investigate unlawful police actions. In the case of assemblies, the Hungarian police have positive obligations to prevent violations of the right to protest and a special responsibility to maintain the peace.

The HCLU is observing that the police often do not operate within the confines of the law upon recording events. They are recording the full duration of almost all gatherings in the capital, even when protesters do not engage in acts of violence or when there is no reasonable basis for gathering evidence towards a potential legal action. In scenarios such as these, their blanket recordings have no meaningful justification.

Moreover, these apparently unlawful police recordings of protesters raise serious concerns about how the recordings are handled afterwards. The Hungarian data protection commissioner recommended[102] that recordings of assemblies be deleted once the police conclude that no rights violations occurred or that no further action will be taken. Subsequently, the Police Act was amended with the requirement that recordings be deleted. Later, a general amendment to the Police Act in 2008 regulated the duration of recordings storage in a more strict and detailed manner: if the police conclude that no right violation occurred and/or no further legal action shall be taken, then footage taken by the police officers shall be deleted after 30 days and CCTV-camera recordings shall be deleted after five days. However, the HCLU has no information regarding whether the police comply with these requirements, and due to its annual reports the Hungarian National Authority for Data Protection and Freedom of Information hasn't yet examined the police practice in this regard.[103]

A recently introduced police practice raises further issues concerning the rights of protesters. Lately, organised protests tend to be prolonged by participants after their official programmes are over. Under Hungarian law, the organiser of a demonstration ceases to bear responsibility for an event after announcing the end of the official programme. Technically, the event finishes at this point. If the participants decide to carry on demonstrating, either at the site of the preceding protest or by marching to other places, their actions are considered to constitute a new, spontaneous demonstration. However, more recently, the police have started to systematically fine these protesters for walking on the

[101] Article 42 of Act XXXIV of 1994 on the police (Police Act)
[102] Recommendation 118/A/1995
[103] This body's annual reports are available at: https://www.naih.hu/annual-reports.html

street and thereby obstructing vehicular traffic.[104] This suggests that the police do not consider the ongoing protests legal. Additionally, the police introduced the practice of surrounding protesters and forcing them to state their names and provide other identifying information while filming.[105] A likely reason for this would be to facilitate identifying people in footage that was indiscriminately recorded before. According to protesters, they are only allowed to leave after complying with the request. The same protesters report receiving fines some weeks after their data was obtained in this way, and some say they were fined for obstructing vehicular traffic despite never leaving the sidewalk.

Obviously, this new police practice has a serious chilling effect on freedom of assembly. It also lacks clear legal grounds: while the law authorises the police to ask for identification documents, and this action can be recorded by the authorities, citizens cannot be forced to link their personal data to their faces in video recordings.

While the police have blanket authorisation to record protests and protesters, in contrast citizens were sanctioned for recording police officers on duty until recently. According to civil court case law, recording police officers without their consent amounted to a violation of their personality rights.[106] While a 2014 Constitutional Court decision overturned this case law, it only allowed members of the press to record police officers and did not include ordinary citizens.[107] This led to ambiguity as to whether protesters are allowed to legally record police officers during demonstrations.

Although the Constitutional Court set forth some important principles regarding the filming of on-duty police officers, private security employees are often those who curtail protesters' rights. Most recently, security guards from the public service media building used excessive force against Members of the Parliament who documented the incident by livestreaming it.[108] According to the head of the National Authority for Data Protection, the MPs violated the guards' privacy rights.[109]

---

[104] In some cases, the court reversed the police decision, see more at: https://tasz.hu/cikkek/akkor-sem-birsagolhato-meg-egy-spontan-tunteto-ha-lelep-a-jardarol

[105] See the last video in this online coverage of a demonstration: https://24.hu/belfold/2018/12/13/tgm-ennek-a-korszaknak-vege/?fbclid=IwAR00cH1uuvkp58ZUvuKZnK5Ul3eW6OiUuH1_brD4OLY34S4Wc2-vXRmankU

[106] Personality rights are an area of civil law in Hungary and seek to protect against violations including defamation, among others.

[107] Decision 28/2014. (IX. 29.) of the Constitutional Court. The English summary of a similar subsequent case, which refers to that decision, is available here: http://www.codices.coe.int/NXT/gateway.dll/CODICES/precis/eng/eur/hun/hun-2016-3-005

[108] See: https://24.hu/belfold/2018/12/17/video-hadhazy-akos-szel-bernadett-kipenderit-allami-televizio-mtva-eroszak-fegyveres-orseg/

[109] See: https://www.hirado.hu/belfold/kozelet/cikk/2019/01/14/naih-az-orszaggyulesi-kepviselokre-is-vonatkozik-az-unio-adatvedelmi-rendelete#

On a final note, since government propaganda is thriving in Hungary, it is increasingly common for leading social protest figures (such as demonstration organisers) to find themselves targeted by smear campaigns. These propaganda articles then sweep through social media, causing enhanced damage to the victims.[110]

3.10 ICCL - Secretive IMSI catcher use in Ireland

Elizabeth Farries, Information Rights Project Manager

One key concern in Ireland is the use of IMSI catchers in the policing of protests and protesting groups, and the potential resultant interferences with and chilling effects on freedom of assembly.

While we are not aware of any official confirmation that IMSI catchers have been used in Ireland,[111] we understand from media reports that some evidence suggests the An Garda Síochána police service (also known as the Gardai) has purchased and used IMSI catchers, and that Garda purchase orders from 2012 show the organisation paid Smith Myers Communications 75,358 euros for 'operational equipment'.[112] Smith Myers is a supplier of IMSI catchers.

The ICCL described in INCLO's 2015 *Surveillance and Democracy* report[113] strong evidence suggesting that the Gardai may have used stingrays to spy on the Garda Síochána Ombudsman Commission. Subsequently, Digital Rights Ireland and Privacy International made 2015 UN submissions on IMSI catchers in Ireland, describing this problem and arguing for criminalisation of IMSI catcher use.[114]

Apart from journalistic or informal sources, it is our understanding that there is no mechanism in Ireland to obtain information about the use of IMSI catchers and other surveillance technology by policing institutions to watch protests.

The ICCL highlighted in our 2018 report on human rights-based reform of policing in Ireland[115] that there is little oversight and no public accountability for surveillance activities by the police or Defence Forces in Ireland. We have expressed similar concerns in INCLO's *Unanswered Questions* report

[110] See for example: Victims must seek judicial remedy: https://ataszjelenti.blog.hu/2019/02/22/te_is_nyerhetsz_pert_a_propaganda_ellen_ha_hazudnak_rolad
[111] The ICCL also emailed Deputy Commissioner John Twomey on 28 February 2019 to ask whether they might provide any information to the ICCL on the use by policing authorities of IMSI catchers at public order or protest operations in Ireland.
[112] Mark Tighe, 'Privacy fears over gardai's "spy" gadget' (*The Sunday Times*, 20 March 2016), available at: https://www.thetimes.co.uk/article/privacy-fears-over-gardais-spy-gadget-gsf3wflhj8m
[113] Available at: https://www.inclo.net/pdf/surveillance-and-democracy.pdf
[114] See Privacy International and Digital Rights Ireland, 'The Right to Privacy in Ireland' (September 2015), paras. 54-56: https://privacyinternational.org/sites/default/files/2017-12/upr_ireland.pdf
[115] ICCL, 'Rights-based Policing: How Do We Get There?'(2018) available at: https://www.iccl.ie/wp-content/uploads/2018/01/RIGHTS-BASED-POLICING-ICCL-submission-to-CFP-2.pdf

on intelligence sharing.[116] In general, there is very little law that applies to surveillance here. According to legislation, the Minister for Justice has sole authority to decide what falls into the category of 'state security' policing. Oversight bodies such as the Policing Authority, Data Protection Commission and Garda Síochána Ombudsman Commission are all exempt from overseeing 'state security' policing.

3.11 KHRC - Surveilling human rights defenders in Kenya

Martin Mavenjina, Programme Assistant, Transitional Justice

In Kenya, numerous instances of unlawful and disproportionate surveillance have come to light in the past few years, most recently before, during and after the 2017 general elections. This trend has become the hallmark of intelligence gathering and sharing by Kenyan security agencies, which continue to be accused of unlawful surveillance of human rights defenders and journalists working on critical issues.[117]

The right to assembly, demonstrations, picketing and to present public petitions to state authorities is enshrined in Kenya's Constitution[118] as well as in several international instruments to which Kenya is a signatory.[119] Kenyan law prohibits digital surveillance; however, certain provisions grant extensive powers to security agencies to limit fundamental freedoms during terrorism-related investigations.[120] Further, the absence of specific legislation or regulations on data protection has given the National Intelligence Service[121] and security agencies in Kenya unfettered discretion to collect data, even when this infringes on citizens' rights to peacefully assemble, picket and demonstrate.

This could explain why most peaceful demonstrations have been forcefully disrupted by police officers from the National Police Service. Human rights defenders and civil society organisations often rely on social media platforms like WhatsApp, email and mobile communications to organise advocacy and peaceful demonstrations on the streets of Nairobi and in other parts of Kenya. These platforms are vulnerable to unlawful surveillance by state agencies. When the

[116] Available at: https://www.inclo.net/pdf/iisp/unanswered_questions.pdf
[117] Critical issues include of impunity in post-electoral violence, extrajudicial executions, counterterrorism, accountability, social auditing, sexual and reproductive health rights, and land rights.
[118] Article 37 of the Constitution of Kenya.
[119] For example, the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR), to which Kenya is a signatory.
[120] The Security Laws Amendment Act 2014 made certain amendments to provisions of the Prevention of Terrorism Act that explicitly enable national security bodies to intercept communications 'for the purposes of detecting, deterring and disrupting terrorism', though this must be authorised by an interception order granted by the High Court.
[121] The National Intelligence Service's primary function has been to gather, collect, analyse and transmit or share with relevant state agencies any security intelligence and counterintelligence, with the aim of detecting and identifying threats or potential threats to national security.

police disrupt these demonstrations, they tend to use crowd-control weapons or, in certain extreme instances, lethal force.

For instance, a peaceful demonstration convened in 2016 by the KHRC and other civil society partners to protest against rampant corruption was brutally dispersed by police officers who lobbed tear gas at the demonstrators even before they could leave Freedom Corner-Uhuru Park, a place associated with Kenya's liberation struggle from colonial rule and repression. There were unconfirmed allegations that security agencies had unlawfully intercepted the demonstration organisers' phone conversations, thus explaining how they had credible intelligence on the protest.

Vocal civil society organisations like Muslims for Human Rights in Mombasa have raised concern over state surveillance of their protest movements and work. They identify this as part of an ongoing trend of intimidating and attacking human rights defenders. In 2015, two organisations accused the Kenyan government of intercepting their communications. The Kenyan government responded with sanctions by listing them as 'specified entities', which meant they were equated with terrorist groups under the Prevention of Terrorism Act[122]. Following this decision by the Kenyan government, the Non-Governmental Organizations Co-ordination Board proceeded to deregister both organisations.[123]

In a further move perceived by civil society actors as a ploy to enhance surveillance of their activities by intelligence and security agencies, the Kenyan government moved the NGOs Co-ordination Board from the Ministry of Devolution and Planning to the Ministry of Interior and Coordination of National Government. This would make such surveillance actions easily justifiable on account of national security.

Since then, there have been many suspected examples of state surveillance technology being deployed against protesters. The National Coalition of Human Rights Defenders – Kenya (NCHRD-K) has, on numerous occasions, received complaints of possible surveillance of human rights defenders by state security agencies. This has occurred in circumstances suggesting that the surveillance is directly related to the rights defenders' work around exercising their constitutional right to assemble, demonstrate, picket and present public petitions to authorities. While concrete evidence of such surveillance may be lacking when these complaints are filed, human rights defenders are apprehensive of surveillance and tracking. About two years ago, before a planned protest in the Kibera neighbourhood of Nairobi, most rights defenders were reportedly called by the police and cautioned against taking part in the protest. More recently, amid a conflict in Laikipia County in 2017, a female human rights defender reported that she had received threats from an Officer Commanding Station

[122] Available at: http://www.kenyalaw.org/lex/actview.xql?actid=No.%2030%20of%202012
[123] This action also affected 508 other NGOs, 15 of which were accused of being a conduit of terrorism.

(OCS) in Samburu for 'being too vocal on the conflict'. This was in the context of her intending to mobilise locals to protest against the state's failure to resolve the conflict which had taken its toll on the predominantly pastoral community. The rights defender believed that her phone calls were being intercepted and her communications were being tracked and surveilled. Separately, in June 2017, the administrative coordinator of the Mathare Social Justice Centre (MSJC) – an organisation that has played a critical role in organising human rights defenders to peacefully protest against systemic rights violations – reported that he was under police surveillance and had been arrested outside his home. This came a month after his organisation released a report on extrajudicial executions in Mathare, following a series of community dialogues in Nairobi.

Over time, security agencies have adopted a strategy that heavily relies on digital surveillance technology in their fight against crime but even more so in their counterterrorism efforts. This strategy has seen the government invest significantly in surveillance technology that includes security cameras, cellular network interception boxes, disclosures from telecommunications providers, and command centres that have granted security agencies expanded authority to conduct digital surveillance.[124]

Legal case

In April 2018, the High Court ruled in *Kenya Human Rights Commission v Communications Authority of Kenya, et al*[125] that the installation of a device management system to access information on subscribers' identities and records[126] with the objective of weeding out counterfeit phones would limit the right to privacy. It therefore held that such a limitation should be done in strict conformity to Article 24 of the Constitution, which provides for limiting fundamental rights and freedoms "under certain extreme circumstances".

[124] The *Track, Capture, Kill* report published by Privacy International in March 2017 disclosed that Safaricom, Kenya's leading mobile internet provider, routinely provided data to authorities without a warrant for intelligence purposes. This report also revealed that national security agencies in Kenya, especially the National Intelligence Service, had unlawful direct access to communication systems in Kenya that allowed for the interception of both data and content (see: https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf). Another report published by the Centre for Intellectual Property and Information Technology Law disclosed that it had detected the presence of a 'middle-box' on a cellular network operated by Safaricom. While middle-boxes have legitimate functions such as network optimisation, they can also be used to manipulate traffic and assist in surveillance. Safaricom denied the existence of the box, and subsequent tests returned negative results, leading the researchers to conclude that it was removed.

[125] Judgment available at: http://kenyalaw.org/caselaw/cases/view/151191/

[126] Specifically, the International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), Mobile Station Integrated Subscriber Directory Number (MSISDN) and the Call Data Records (CDRs) of subscribers.

3.12 LRC - Police use grabbers against protesters in South Africa

Sherilyn Naidoo, Openness and Accountability Attorney

In 2016, evidence surfaced that South African Intelligence was using technology such as grabbers and other software to watch protesters and activists' online activity.[127] However, given that the South African government and intelligence agencies have not explicitly admitted to these activities, the extent of this surveillance is unknown.

South Africans became aware of the possible use of grabbers in July 2015 when several individuals were arrested in a police sting by the South African Hawks (the crime unit in charge of investigating priority and organised crimes as well as serious commercial crimes and corruption) while trying to privately sell a grabber. Several media reports carried on- and off-the-record comments by police sources that strongly suggested[128] that governmental agencies had bought and presumably used such technology themselves. Further evidence of police use of grabbers was detailed in an investigative report in the *Mail & Guardian* newspaper.[129]

While regulations issued under the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) prohibit the private use, sale or possession of such technology, RICA is silent on the state's use of such devices. It is not clear if police apply for judicial authorisation when using a grabber device, and information requests made by the Right2Know Campaign in South Africa to verify this were refused.[130] However, as grabbers are capable of mass surveillance – which is unregulated by RICA or any law – it is unclear if the use of such devices is lawful at all.[131]

In November 2015, Parliament's Joint Standing Committee on Intelligence stated that it intended to 'revisit RICA with a view of whether any changes would be required to strengthen the Act in the likely event that the Judge is not sufficiently empowered to deal with matters such as grabbers.'[132] As a result, there is

---

[127] Marianne Thamm, 'National police commissioner turns to court to flush out info on ANC vote-buying scandal' (*Daily Maverick*, 11 January 2019) available at: https://www.dailymaverick.co.za/article/2019-01-11-national-police-commissioner-turns-to-court-to-flush-out-info-on-anc-vote-buying-scandal/

[128] Solly Maphumulo, 'Hunt for "super-spy" machines' (*IOL*, 27 August 2015) available at: https://www.iol.co.za/news/hunt-for-super-spy-machines-1906508#.Vd7X7nvV_BE

[129] Heidi Swart, 'How cops and crooks can "grab" your cellphone - and you' (*Mail & Guardian*, 27 November 2015) available at: https://mg.co.za/article/2015-11-29-how-cops-and-crooks-can-grab-your-cellphone-and-you

[130] For more on the R2K Campaign, see: http://www.r2k.org.za/2015/09/03/surveillance-device/

[131] See Right2Know Campaign and Privacy International, 'The Right to Privacy in South Africa' (October 2016) available at: https://privacyinternational.org/sites/default/files/2018-04/South%20Africa_UPR_Stakeholder%20Report_Right%20to%20Privacy.pdf

[132] Parliamentary Joint Standing Committee on Intelligence, available at: http://www.parliament.gov.za/live/content.php?Item_ID=8495

evidence of the use of grabbers in South Africa. However, its lawfulness and the extent to which they are used by our agencies are unclear. It is suspected that grabbers have been used to watch activists, protesters and journalists, but there was no adequate proof of such until recently.

Surveillance of student protesters in the #feesmustfall movement

South African investigative journalist Jacques Pauw first exposed the possible surveillance of student protesters by South African Intelligence in his book *The President's Keepers*.[133] There has been further speculation that the phones and social media of student protesters during the 2016 #feesmustfall movement were also watched. Until recently there was no evidence to prove this. In a matter related to the South African Independent Police Investigative Directorate (IPID) investigation of tender fraud and corruption, the South African national police commissioner approached the Pretoria High Court to order a magistrate to hand over records that were considered when subpoenas were issued against various state actors in the investigation.[134] The High Court granted access to these records. They revealed that there was an alleged procurement from a company called iView, which was not on the governmental database as a supplier, to procure a 45 million rand grabber. These records also revealed that the company had allegedly been paid for an encryption application called Daedalus to watch social media sites during the #feesmustfall student protests. These records provide us with evidence that South African Intelligence is using technology such as grabbers and other software to watch protesters and activists.[135] The extent of this surveillance is unknown.

3.13 Liberty - Use of face surveillance by UK police forces

Hannah Couchman, Policy and Campaigns Officer

Since 2015, three police forces in the United Kingdom have used Automated Facial Recognition (AFR) technology, a form of face surveillance, in live public settings – South Wales Police (SWP), the Metropolitan Police (the Met) and Leicestershire Police. SWP and the Met continue to use AFR. The Met's initial trials concluded in January 2019 and a wider operational rollout will now be discussed, while 'pilots' carried out by SWP are ongoing with no end date specified.

[133] Jacques Pauw, *The President's Keepers* (NB Publishers 2017).
[134] Marianne Thamm, 'National police commissioner turns to court to flush out info on ANC vote-buying scandal' (*Daily Maverick*, 11 January 2019) available at: https://www.dailymaverick.co.za/article/2019-01-11-national-police-commissioner-turns-to-court-to-flush-out-info-on-anc-vote-buying-scandal/
[135] Marianne Thamm, 'National police commissioner turns to court to flush out info on ANC vote-buying scandal' (*Daily Maverick*, 11 January 2019) available at: https://www.dailymaverick.co.za/article/2019-01-11-national-police-commissioner-turns-to-court-to-flush-out-info-on-anc-vote-buying-scandal/

AFR technology works by scanning the faces of all passers-by in real time. The software measures their biometric facial characteristics, creating unique facial maps in the form of numerical codes. These codes are then compared with those of other images on bespoke police watchlists. There is little transparency around who is included on the watchlists and where the images are obtained from. While some images are likely to be drawn from the Custody Images Database, which contains the images of thousands of people who have never been convicted of a crime, they may also be taken from social media or from other surveillance. The watchlists are not limited to people wanted for crimes, and have previously included people with mental health conditions.[136]

SWP has been at the forefront of AFR deployment, receiving 2 million pounds from the Home Office to 'trial' the technology. It has used this technology at least 23 times since May 2017. SWP has used AFR technology at a range of events, including music festivals and sports matches, and at shopping centres. On 27 March 2018, SWP used AFR technology for the first time at a protest, specifically at a peaceful protest outside Cardiff Arms Fair. Protesters have told Liberty how the AFR van was parked up alongside protesters in an intimidating fashion; they said it looked as though it was designed to discourage protest. The protesters were not aware that AFR technology would be deployed, and the police did not provide any information at the time of the event. Some protesters have indicated that they would be put off attending future protests if AFR technology is used. They described feeling watched or tracked – a stark example of the chilling effect of face surveillance.

Use of AFR technology is not authorised by any law, and the government has not provided any policies or guidance on it. No independent oversight body regulates its use either. Shockingly, AFR technology has been found to disproportionately misidentify women and black, Asian and minority ethnic people, meaning they are more likely to be wrongly stopped by the police and have their images and biometric data stored.[137]

Legal case

Liberty is representing Ed Bridges, an activist in South Wales who attended the Cardiff Arms Fair protest, in his legal challenge against SWP. Ed is challenging the lawfulness of SWP's use of AFR technology and is calling for an immediate end to its use in public spaces. The case will be a nationwide test of the state's power to deploy biometric surveillance tools.

---

[136] For example, at Remembrance Sunday commemorations in London in November 2017, the Met compiled a watchlist of images of people with known mental health issues. SWP and the Met have also admitted that images could come from social media.

[137] See Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (*Proceedings of Machine Learning Research*, vol. 81, 2018): http://proceedings.mlr.press/v81/buolamwini18a.html; see also Brendan F. Klare et al, 'Face Recognition Performance: Role of Demographic Information' (*IEEE Transactions on Information Forensics and Security*, vol. 7, issue 6, December 2012): https://ieeexplore.ieee.org/document/6327355

A key focus of Ed's challenge is the way that SWP's use of AFR technology interferes with freedom of expression and protest rights (Articles 10 and 11 of the European Convention on Human Rights, or ECHR). AFR technology has a chilling effect on people's attendance of public events and peaceful protests, and their behaviour while there. The presence of an AFR van at a protest means that protesters are being watched and can be identified, tracked and marked for further police action. Ed is also challenging SWP's use of AFR technology on the grounds that it violates the general public's right to privacy (Article 8 of the ECHR) by indiscriminately capturing (and potentially storing) the personal biometric data of everyone within the camera's range, and that it breaches UK data protection and equality laws.

Liberty's application has not been contested by SWP. We have now received permission in the case and it will be heard in due course.

i Terms glossary

Automated Facial Recognition (AFR)

AFR technology works by scanning the faces of all passers-by in real time. The software measures their biometric facial characteristics, creating unique facial maps in the form of numerical codes. These codes can be compared with those of other images.

Face Surveillance

Surveillance technology capable of identifying or verifying a person from a digital or video image or source. It can scan the faces of all passers-by in real time. The technology measures biometric facial characteristics, creating unique facial maps in the form of numerical codes. These codes are then compared with those of other images.

IMSI catchers

Often described as 'stingrays' or 'grabbers', IMSI catchers are a class of surveillance devices that provide active online interception capabilities. Citizenlab calls them 'cell site simulators' and says they mimic the strongest nearby cell phone tower to which our personal communications devices, including our mobile phones, connect. This connection allows the IMSI catchers to obtain identifiers that policing institutions use to secretly watch how we operate our personal devices.

Online protest

A tenuous term which attempts, perhaps unsuccessfully, to distinguish protest in online and offline spaces. However, when we consider how protest manifests in our digital age, we acknowledge that the continuity and interplay between online and offline protest. Laws applied in offline spaces impact behaviour in online spaces, and policing institution actions in online spaces can have offline consequences. Therefore, rather than engaging in the legally complex challenge of separating, isolating and defining the concept of 'online' protest in distinction to its supposed counterpart, INCLO has chosen instead to identify the types of online surveillance technologies that are used to deter protesters, in online and offline spaces alike.

Online surveillance technologies

Technologies designed to watch, intercept, record, retain, analyse and disseminate personal data online. By 'online' we do not refer only to web-based, internet-run or open sources, but also to diverse technologies that are connected via intranets restricted to the exclusive use of state agencies, as happens with intelligence software. They are deployed by policing institutions against

protesters – often without our knowledge, our consent, or available legal avenues of recourse. This can disrupt and preclude our ability to gather and speak out and thus interfere with our rights to assemble and dissent, in online and offline spaces alike.

Open sourced intelligence

An alternative term for social media networks whose privacy controls are made public and which are used as an information source by policing institutions. It is increasingly common for policing institutions to receive state training on how to engage protesters and track their online activities.

Pineapples

First released in 2008 by Hak5, Pineapples allow easily executable attacks on public Wi-Fi networks. They use multiple radios and can therefore interface with hundreds of devices at a time and are optimised to execute complicated network attacks.

Policing institutions

Those state agencies and law enforcement agents (excluding non-state actors) tasked with the responsibility for safety, security and the protection and promotion of the rights to protest.[138]

Protesters

Activists, organisers and individuals who participate in protests.

Protests

INCLO's use of the term 'protest' follows that of the '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', UN Doc. A/HRC/31/66 (4 February 2016), para. 10: '[A]n intentional and temporary gathering in a private or public space for a specific purpose, and can take the form of demonstrations, meetings, strikes, processions, rallies or sit-ins with the purpose of voicing grievances and aspirations or facilitating celebrations.'

The SORM system

In Russia, the 'System for Operative Investigative Activities' (known as SORM) is the technical foundation for targeted mass communication surveillance. Communications service providers are obliged to install at their own expense a special device ('Punkt Upravlenia') on their networks that allows the Federal Security Service (FSB) to directly collect traffic without the knowledge or co-

[138] See more in our *Defending Dissent* report, available at: https://www.inclo.net/pdf/Defending-Dissent-Report-Complete-WEB-FINAL.pdf

operation of the service provider. The FSB tracks behaviours including credit card transactions and other web use including social networks, chats and forums.

ii About INCLO

INCLO is a network of 13 independent, national human rights organisations across the globe. We work together to promote fundamental rights and freedoms. Together we are: 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 (EIPR), the Human Rights Law Network (HRLN) in India, the Hungarian Civil Liberties Union (HCLU), 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.

We support and mutually reinforce the work of member organisations in their respective countries and collaborate on a bilateral and multilateral basis. INCLO works on four thematic issues: (1) protest rights and policing; (2) surveillance and human rights; (3) religious freedom and equal treatment; and (4) protecting civic space.

Regarding protest rights, policing and surveillance, INCLO is a recognised voice in regional and international forums. Our comprehensive research reports on matters related to protest and surveillance include:

- *Defending Dissent: Towards State Practices that Protect and Promote the Rights to Protest* (2018) https://www.inclo.net/pdf/Defending-Dissent-Report-Complete-WEB-FINAL.pdf
- *Lethal in Disguise: The Health Consequences of Crowd-Control Weapons* (2016) https://www.inclo.net/pdf/lethal-in-disguise.pdf
- 'The Right to Privacy in the Digital Age' - Submissions towards the Office of the High Commissioner on Human Rights regarding Human Rights Council adopted resolution 34/7 (2018) https://www.inclo.net/pdf/ohchr-en.pdf
- *Surveillance and Democracy: Chilling Tales from Around the World* (2016) https://www.inclo.net/pdf/surveillance-and-democracy.pdf
- *Take Back the Streets: Repression and Criminalization of Protest Around the World* (2013) https://www.inclo.net/pdf/take-back-the-streets.pdf
- *Unanswered Questions - International Intelligence Sharing* (2018) https://www.inclo.net/pdf/iisp/unanswered_questions.pdf
- *Call for action – Regulate Intelligence Sharing* (2018 with Privacy International) https://www.inclo.net/pdf/Intelligence-Sharing-Brochure-WEB.pdf

Learn more at https://inclo.net