The surveillance industry and human rights: Submission to the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression by the Association for Progressive Communications (APC)

May 2019

1. About APC

The Association for Progressive Communications (APC) is an international network and non-profit organisation founded in 1990 that works to help ensure everyone has affordable access to a free and open internet to improve lives, realise human rights and create a more just world. As an organisation that has worked at the intersection of human rights and technology for nearly three decades, we welcome the opportunity to contribute to the Special Rapporteur on the right to freedom of opinion and expression's work on the surveillance industry and human rights.

2. Introduction

In 2018 the United Nations General Assembly (UNGA) affirmed that the "surveillance of digital communications must be consistent with international human rights obligations" and in accordance with a "publicly accessible, clear, precise, comprehensive and nondiscriminatory" legal framework, without any arbitrary or unlawful interference with the right to privacy. UNGA called on states and business enterprises to protect and respect the right to privacy in the digital age in accordance with their respective responsibilities under international human rights law.[1]

There is a stark difference between the normative statements expressed in UN resolutions and the realities experienced by individuals and communities on the ground across the globe. Individuals feel increasingly surveilled in multiple ways, including targeted, mass and lateral surveillance, with little knowledge on who is carrying out this surveillance or how. As noted by an activist at a recent consultation on the topic, "We feel like we are performing on a stage, with no knowledge of who the audience is."[2] The "curation" of these clandestine performances can often be credited to the surveillance technology industry, which behind the scenes is collecting, retaining, processing and exploiting data for governments, other companies, and other non-state actors willing to purchase a ticket.

To a large extent, people are in the dark as to the different tools available to and being produced by state and non-state actors (especially private sector) that are used for surveillance purposes.

There is limited public information concerning the surveillance technology industry, which makes it difficult to hold either governments or private companies accountable for deploying surveillance technologies in ways that are inconsistent with international human rights law as well as domestic law. While surveillance technologies may have legitimate uses and be designed "neutrally", the reality is that they are deployed in ways that violate a range of human rights with impunity. Furthermore, as the Special Rapporteur has already recognised:

> Surveillance exerts a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, members of certain political parties, civil society, human rights defenders, professionals such as journalists, lawyers and trade unionists, victims of violence and abuse, and children.[3]

The same can be said for surveillance technologies. Whether targets of government surveillance (like activists, human rights defenders, journalists whose communications and devices are intercepted) or subjects of lateral/social surveillance (like survivors of domestic violence who are targeted with spousal spyware and experience new forms of domestic violence through "internet of things" devices), persons who are in positions of vulnerability and marginalisation in society, including political dissidents, minority rights activists, persons living in conflict areas and women or persons of varying gender identity, tend to experience disproportionate effects from the deployment of surveillance technologies.

Due to the limitations on space, our submission will focus on emblematic cases and uses of surveillance technologies against individuals or civil society organisations, and the gendered impact of the deployment of surveillance technologies.

[1] https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/179

[2] Quote from a participant at the regional consultation "Trends and Trajectory of the Shrinking Civic Space in Asia", Bangkok, December 2018.

[3] http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/32/38&Lang=E

3. Emblematic cases of state use of private surveillance technology against individuals or civil society organisations

Unfortunately, there is no shortage of examples of states using surveillance technology against human rights defenders and civil society society organisations. A range of technologies – some designed for surveillance purposes, others not – are used by the state for this purpose, including spyware, facial recognition technologies, financial surveillance, closed circuit TV (CCTV), internet service providers, data mining tools, drones, internet of things devices, smart cities, international mobile subscriber identity (IMSI) catchers, and biometric identification systems, among others.

Spyware to monitor civil society actors (including HRDs): Highly intrusive software applications used to track communications, known as spyware, have been found to be deployed in dozens of countries in every region of the world.[4] Ostensibly designed and sold for the purpose of preventing crime and terrorism, tools like NSO Group's Pegasus can turn a phone into a powerful surveillance tool, enabling an operator to extract text messages (including encrypted messages), contact lists, photos, calendar records, emails, instant messages and location, as well as to turn on microphones and cameras, enabling them to capture live footage and record conversations.[5]

Another popular spyware, Remote Control System (RCS), developed by Hacking Team, gives an operator access to a target's computer or mobile phone, allowing them to copy files, VoIP calls, emails, instant messages and passwords as well as access a device's camera and microphone to spy on its owner and those in close proximity.

These highly intrusive tools can and have been used to target human rights defenders, civil society organisations, journalists and others, such as Ahmed Mansoor in the United Arab Emirates,[6] proponents of a soda tax as well as other activists and journalists in Mexico,[7] activists and opposition political leaders in Bahrain,[8] Amnesty International,[9] and Omar Abdulaziz, a Canada-based Saudi activist who was in direct communication with the murdered Saudi journalist Jamal Khashoggi,[10] among others. The companies behind these leading spyware products include FinFisher, Hacking Team and NSO Group, companies based in Europe and Israel. These products are sold to governments that have demonstrated their propensity to violate human rights, including through their surveillance practices.

Social media intelligence: Social media intelligence (SOCMINT)[11] refers to the techniques and technologies that allow companies or governments to monitor social media. SOCMINT can be a highly intrusive practice used to violate the privacy of individuals, infiltrate civil society organisations and

[4] See https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/ and https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

[5] https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-asmartphone.html?module=inline

[6] https://foreignpolicy.com/2016/08/25/the-uae-spends-big-on-israeli-spyware-to-listen-in-on-a-dissident/

[7] https://www.nytimes.com/2018/02/20/world/americas/mexico-spyware-investigation.html, https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html, https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html

[8] https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation

[9] https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/

[10] https://www.washingtonpost.com/world/middle_east/khashoggi-friend-sues-israeli-firm-over-hacking-he-sayscontributed-to-the-journalists-murder/2018/12/03/ddcb28ee-f708-11e8-8642c9718a256cbd_story.html?utm_term=.9f0dee6c2bda

[11] https://www.privacyinternational.org/explainer/55/social-media-intelligence

social networks, and generally create a chilling effect for freedom of expression. Some examples of companies providing SOCMINT technologies include NICE, Ntrepid, Kapow Software, Media Sonar, Geofeedia, Snaptrends and Cogito. A South African company called VASTech makes a tool called "The Badger" available for surveilling social media.[12] Increasingly, government agencies are turning to tools designed for marketing purposes in order to reduce costs.[13] Some examples of states engaging in SOCMINT include the following:

- In 2015 the Israeli state attorney's office started operating the "Cyber Unit", a unit responsible for "dealing with cyberspace enforcement challenges" via the censorship of social media posts.[14] The unit has developed a "predictive policing system" to monitor Palestinians' social media posts.[15] This system has resulted in content removal and arrests of innocent people, such as young Palestinians, journalists, activists, human rights defenders and children. For example, in October 2017, Israeli forces arrested a Palestinian worker for posting "good morning" in Arabic on his Facebook account, which the automatic translations of Facebook mistakenly translated to "attack them" in Hebrew and "hurt them" in English.
- In 2018, India's Ministry of Information and Broadcasting[16] published a bid for the development of a "social media analytical tool" that would create digital profiles of citizens, ostensibly to gauge their opinions about official policies. The tool, according to the specifications of the bid document,[17] would have the capacity to monitor a range of digital platforms: Twitter, YouTube, Instagram and blogs. The tool would also be required to "listen to" email. This was supposedly aimed towards gauging public sentiment and promoting "positive consensus" on state policies. Following public outcry, the government withdrew its proposal; however, multiple state agencies have been systematically monitoring data and activities of individuals online.[18] The state had earlier set up "Social Media Monitoring Hubs", which was deemed unconstitutional by the Supreme Court, observing that India is turning into a surveillance state.[19]
- In the United States, Media Sonar software was used to monitor social media platforms like Facebook, Twitter, Instagram and Flickr. In 2016, the American Civil Liberties Union found that it was helping the police to use hashtags such as #BlackLivesMatter and #DontShoot to monitor protesters. In reaction, Twitter and Facebook cut Media Sonar's access to their data.[20]

Infrastructure: Control over ICT infrastructure can be a powerful tool for state surveillance. It has allowed Israel, for example, to conduct mass surveillance of Palestinians and restrict their access to digital rights.[21] While there are severe limitations on the surveillance of Israeli citizens, Palestinians are

[12] https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf

[13] Ibid.

[14] https://www.adalah.org/en/content/view/9228

[15] https://www.opendemocracy.net/en/north-africa-west-asia/israeli-algorithm-criminalizing-palestinians-for-o/

[16] https://scroll.in/article/879833/government-plans-to-monitor-individual-social-media-users-to-gauge-opinion-aboutofficial-policies

[17] www.becil.com/uploads/tender/TendernoticeBECIL01pdf-04836224e38fdb96422221c4e057f6c5.pdf

[18] https://www.medianama.com/2018/09/223-40-government-departments-are-using-a-social-media-surveillance-toolscroll-in/

[19] https://www.indiatimes.com/news/india/govt-slammed-for-social-media-monitoring-sc-says-india-is-becoming-asurveillance-state-349302.html

[20] https://www.dailydot.com/layer8/media-sonar-twitter-social-media-monitoring/

[21] https://www.apc.org/en/pubs/%E2%80%9Cconnection-interrupted-%E2%80%9C-7amleh-center-digital-occupationpalestinian-telecommunications

not afforded this protection.[22] Furthermore, Israel's ability to send automated phone calls and text messages through Palestinian networks – for example, to Palestinians in Gaza during its military offensives – is an example of how Israel can collect and intercept Palestinian communications, violating their right to privacy and operating without any transparency or accountability.[23] The extent to which private actors support or are involved in these actions is difficult to establish.

From the South African context we are aware of tools that have been developed specifically for surveilling communications at the infrastructure level, for example, VASTech's satellite signal analyser.[24] For more detail on how VASTech's products are being used, refer to the R2K and ALT Advisory submission to this call for input from the Special Rapporteur.[25]

Surveillance in public spaces: States are also deploying an array of surveillance technologies in public spaces, which are used against civil society, including peaceful protesters.[26] A few examples include drones to surveil protests; facial recognition software in public gatherings, including protests, concerts, sporting events, shopping centres and festivals; and "stingrays"[27] or IMSI catchers, which are deployed to track suspects, but can gather information about the phones of countless bystanders, including protesters.[28] Artificial intelligence (AI) can be used in concert with drone footage or other sources of data.[29]

Facial recognition software and databases are particularly problematic, as has been the case in China where religious minorities have been surveilled[30] and in "safe city" projects in Canada[31] and Pakistan. The deployment of surveillance technology in public spaces often happens in the absence of legal frameworks and presents a range of human rights risks, in particular the rights to peaceful assembly and association and privacy.[3232]

Biometric ID: With many countries implementing or planning large biometric ID systems, fear of mass surveillance and loss of control over identity prevails. While the Supreme Court of India upheld the constitutionality of the Indian biometric ID programme, it has warned about the security concerns. Civil society has repeatedly cautioned about the prospect of such programmes being used for mass surveillance.[33] Biometric systems are increasingly being used, and often with the support of private sector vendors, which makes it critical to ensure that there is transparency and checks and balances on how the data is being obtained, managed and stored. There must be robust oversight of business

[22] Full text of the letter available at: https://goo.gl/Dxd789

[23] https://goo.gl/8CKf8v

[24] https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf

[25] https://www.r2k.org.za/wp-content/uploads/Submission-The-Surveillance-Industry-and-Human-Rights-ALT-Advisoryand-R2K.pdf

[26] https://www.apc.org/en/pubs/rights-freedom-peaceful-assembly-and-association-digital-age-apc-submission-unitednations

[27] https://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/

[28] https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices

[29] https://www.washingtonpost.com/news/the-switch/wp/2018/05/22/amazon-is-selling-facialrecognition-to-law-enforcement-for-a-fistful-of-dollars/?noredirect=on&utm_term=.32800603aefb

[30] https://www.engadget.com/2019/02/17/chinese-surveillance-company-tracks-2-5-millionpeople/?utm_campaign=fullarticle&utm_medium=referral&utm_source=inshorts

[31] https://www.theguardian.com/world/2018/oct/23/toronto-smart-city-surveillance-ann-cavoukian-resigns-privacy

[32] https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/ and https://www.cfr.org/blog/exporting-repression-chinas-artificial-intelligence-push-africa

[33] https://www.apc.org/en/pubs/apc-calls-strong-data-protection-safeguards-following-supreme-court-indias-verdictaadhar

involvement in this process. While biometric ID systems themselves present risks to human rights, in combination with surveillance in public spaces they are particularly concerning.

4. Gender and surveillance

Specific focus is needed on the gendered experience of surveillance. Surveillance is differently experienced by people and communities in positions of marginalisation and vulnerability, and therefore the surveillance industry puts them at disproportionate risk. Examples of people and groups who might find themselves targeted by the surveillance technologies outlined above include women, people of varying gender identities and sexual orientation, and people who face intersecting forms of discrimination based on their ethnicity, caste, religion, economic class, race or age.

Surveillance of women is closely linked to how patriarchy has historically controlled their lives and choices, for instance, in relation to abortion, choice of who to marry, clothes and their mobility. The increased modes by which technology keeps track of bodies and data leads to situations that could pose different levels of risk for women, ranging from being exposed by an ex-partner to situations of physical risk and harm from family and others, to increased tracking by companies and governments in relation to fertility and other health data. This is entirely because devices and applications are not designed with privacy as a default, but rather to allow for surveillance. There is a growing range of ubiquitous technologies and things that can be used for domestic abuse and violence, and the design of devices does not take into account the potential for their use in abuse and violence against women.[34]

The surveillance industry largely conforms to the mainstream and normative in terms of what bodies should look like and the link between biological sex and gender, which vastly differs from the lived experience of many people across the world. This in turn leads to daily and continuous violations of the rights of trans people, whether at work, within family, in public spaces and in private relations in the context of abuse. The existing array of discrimination and exclusion faced by trans people, and also by women and vulnerable groups, put them at further risk from the surveillance industry,[3535] and potentially from the further use of algorithms and automation that will deepen inequalities and biases rather than eradicate them and from experiments connected to big data and surveillance, such as predictive policing already taking place in North America.[36] Massive latent data collection by the surveillance industry allows for companies and governments to use sophisticated and opaque algorithms and computational modelling.

In Tanzania, a member of the government openly declared that a 17-member surveillance team was going to identify phones that have sexual content and social media groups or texts that were promoting "gay behaviour or prostitution".[37] Moves such as these indicate that the companies holding private and personal data collaborate with governments to target citizens who are entitled to protection of their personal autonomy.

[34] https://www.ucl.ac.uk/research/domains/collaborative-social-science/social-science-plus/IOT-outcomereport and https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html
[35] https://jods.mitpress.mit.edu/pub/costanza-chock
[36] https://www.aclu.org/other/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racialjustice
[37] https://www.genderit.org/feminist-talk/melt-down-protections-data-and-privacy-tanzania-lgbtqia-and-others

Netsweeper's filtering technology is often used to limit and block access to certain websites that might be deemed inappropriate This often leads to censoring of content generated by or about LGBTIQ communities.[38] A report published by Citizen Lab[39] has identified the use of this technology in 30 states. The list of blocked pages is extensive and includes LGBT news and culture sites, HIV/AIDS organisations, and advocacy organisations like the International Lesbian, Gay, Bisexual, Trans and Intersex Association.

There is significant gender-based violence faced by women largely in the context of family and intimate relationships, and in relation to surveillance there are an increasing number of tools and applications[40] that allow for surveillance of women within the home. In the context of North America, these have also been used in situations of domestic violence.[41] Applications like Absher also make it possible for men to track the movement of women in Saudi Arabia.[41] Often these are carried out in the name of keeping girls and women safe, with little thought paid to their informed consent or autonomy.

5. Private sector and international organisations

Partnerships entered into and close relations of the private sector entities developing such technologies with governments and bodies such as the United Nations show their deep nexus and the lack of accountability at all levels.[42] This became particularly problematic with the partnership between the UN and Plantir.[43] Experts have warned that these collaborations, if done without adequate oversight, can create ethical issues and expose vulnerable people's data to surveillance and appropriation by powerful interests.[44] Similarly, the extensive use of proprietary software and solutions provided by entities like Microsoft, which have been targets of multiple leaks, calls for similar concern.

6. Recommendations

- States should ensure that the technologies purchased and the way they are used are human rights-compliant and have public oversight.
- States should ensure that these technologies are not used to target dissent or vulnerable groups such as religious and gender minorities.
- There must be periodic review by independent expert bodies on the use and impact of these technologies.
- Frameworks and standards for accountability must be developed for the surveillance technology industry (domestic and international) to prohibit arbitrary and unlawful surveillance.
- A register of entities developing such technologies must be maintained with periodic vetting to ensure compliance with standards.

[38] https://www.openglobalrights.org/identities-in-the-crosshairs-censoring-LGBTQ-internet-content-around-the-world
[39] https://citizenlab.ca/2018/04/planet-netsweeper
[40] https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html
[41] https://www.nytimes.com/2019/02/13/world/middleeast/saudi-arabia-app-women.html
[42] https://www.irinnews.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp
[43] https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world
[44] https://slate.com/technology/2019/02/palantir-un-world-food-programme-data-humanitarians.html

- Robust data protection frameworks that will be applicable to the use of such technologies should be adopted to ensure the protection of the right to privacy and other rights.
- States and the private sector must uphold their respective responsibilities under the UN Guiding Principles on Business and Human Rights.
- UN agencies should conduct human rights impact assessments (with input from affected communities) when procuring technology that can be used for surveillance purposes.
- Experts and civil society must engage in more evidentiary research on the use and development of these technologies, the findings of which should be effectively communicated to all stakeholders.
- Bodies including judiciary and national human rights institutions must be trained to understand and address the use of these technologies.