14 June 2022 Reference: TIGO IOR 40/2022.3017

THE RIGHT TO PRIVACY IN THE DIGITAL AGE

SUBMISSION TO THE OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS FOR THE REPORT ON THE RIGHT TO PRIVACY IN THE DIGITAL AGE

INTRODUCTION

Amnesty International submits the following document inputs for the United Nations High Commissioner for Human Rights' report on the right to privacy in the digital age (2022). The document builds on Amnesty International's informal paper from 2021 which recommended elements to be included in the resolution on the right to privacy due to be negotiated at the 48th session of the UN Human Rights Council. It includes two new areas of interest; Web3 and Neurotechnology.

CYBERSURVEILLANCE TECHNOLOGY

Unlawful targeted surveillance, through for example spyware attacks, violates the right to privacy and the rights to freedom of expression, opinion, association, and peaceful assembly, which are protected by both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

Amnesty has highlighted the global scale of human rights abuses involving cyber surveillance companies, like NSO Group, and its governments clients.[1] We have argued in favour of the need to implement a global moratorium on the export, sale, transfer, and use of targeted surveillance technology until a human rights compliant regulatory framework is in place.

The Pegasus Project, an international investigation bringing together 18 media outlets and Amnesty International as the technical partner, has revealed how NSO Group appears to be complicit in human rights violations and abuses around the world systemically and on a large scale.[2] The Pegasus Project revealed how no one is save from potentially being targeted, including human rights defenders, activists, journalists and even government officials and parliamentarians. Civil society is so rampantly monitored with little to no safeguards and even diplomats and heads of states themselves were potential targets. This should serve as a long overdue wake-up call for legislatures worldwide to step up and regulate this industry.

While NSO Group claims its spyware is only used for criminal and terror investigations, it has become clear that its technology facilitates systemic abuse. As the UN High Commissioner for Human Rights has said, "if the recent allegations about the use of Pegasus are even partly true, then that red line has been crossed again and again with total impunity."[3]

Given the breadth and scale of the findings of the Pegasus Project, there is **an urgent need to halt surveillance technology enabled activities of all states and companies, until human rights regulatory efforts catch up**. In a statement issued on 12 August 2021, a group of Special Procedures warned that "it is highly dangerous and irresponsible to allow the surveillance technology and trade sector to operate as a human rights-free zone," and urged the international community

[1] Amnesty International, *Scale of secretive cyber surveillance 'an international human rights crisis' in which NSO group is complicit',* (23 July 2021) https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-spyware-digital-surveillance-nso-2.

[2] Amnesty International, *Massive data leak reveals Israeli NSO group's spyware used to target activists, journalists, and political leaders globally*, (19 July 2021) https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/

[3] Office of the High Commissioner for Human Rights (OHCHR), *Use of spyware to surveil journalists and human rights defenders statement by UN High Commissioner for Human Rights Michelle Bachelet*, (Press Release: 19 July 2021) https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27326&LangID=E.

"to develop a robust regulatory framework to prevent, mitigate and redress the negative human rights impact of surveillance technology and pending that, to adopt a moratorium on its sale and transfer."[4] This warning followed a call for an immediate moratorium on the sale, transfer and use of surveillance technology by a group of 146 civil society organizations and 28 independent experts, issued on 27 July 2021.[5]

Alongside the impact on the Right to Privacy, the unchecked use of targeted surveillance technologies is shrinking the space for human rights work, and fast exacerbating digital threats against human rights defenders that are spilling over to the offline world. Journalists, activists, and human rights defenders are especially vulnerable to this. States must commit to conducting immediate, independent, transparent and impartial investigations of any cases of unlawful surveillance and where appropriate, pursue legal avenues to provide remedies to victims and hold perpetrators to account, in accordance with international human rights standards.

In this regard, we propose the following recommendations:

- That the UN recognises "that international human rights law requires all States to adopt robust domestic legal safeguards that are in line with international human rights law to protect individuals from unlawful surveillance, invasion of their privacy or threats to their freedom of expression, assembly and association."[6]
- That states, pending the development of the necessary regulatory framework, adopt a global moratorium on export, sale, transfer and use of surveillance technologies.
- That states adopt and enforce a legal framework requiring private surveillance companies and their investors to conduct human rights due diligence in their global operations, supply chains and in relation to the end use of their products and services. Under this legislation, private surveillance companies should be compelled to identify, prevent, and mitigate the human rights-related risks of their activities and business relationships.

FACIAL RECOGNITION AND REMOTE BIOMETRIC RECOGNITION TECHNOLOGIES

Facial recognition technology (FRT) for identification is a mode of mass surveillance, and as such is a violation of the right to privacy and cannot represent a necessary or proportionate interference with the right in any circumstances.

While real-time facial recognition endangers passive individuals being monitored by cameras, and puts their privacy at risk without due cause, facial recognition software for identification where images are compared to a database of thousands of images is, by design, incompatible with the right to privacy. These systems rely on large databases containing millions of images, many scraped from social media and other databases without the user's consent – this is mass surveillance. Imagery from any camera, regardless of its age, can be fed into facial recognition software and matched with this database. The technology also undermines the rights to freedom of expression, freedom of peaceful assembly and association, and equality and non-discrimination.

Furthermore, research has consistently found that FRT processes some faces more accurately than others, depending on key characteristics including skin colour, ethnicity and gender.[7] FRT classification and categorisation is limited and does not allow for nuance – for example, FRT may assign a face with a probability score for being male or female (with varying degrees of success in terms of accuracy) but will struggle to accurately identify non-binary or genderfluid identities. Even when the technology is 'accurate' it can, and is, being used by states to intentionally target certain individuals or groups of

[4] OHCHR, *Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech,* (Press Release: 12 August 2021) https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27379&LangID=E.

[5] Amnesty International, *Joint open letter by civil society organisations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology*, (27 July 2021), https://www.amnesty.org/en/documents/doc10/4516/2021/en/#:~:text=July%2027%2C%202021Index%20Number%3A%20DOC%2010%2F4516%2F2021%20Business%20and,the%20sale%2C%20transfer%20and%20use%20of%20surveillance%20technology.

[6] OHCHR, *Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech,* (Press Release: 12 August 2021) https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27379&LangID=E.

[7] Amnesty International, *Amnesty International calls for ban on the use of facial recognition technology for mass surveillance*, (11 June 2020), https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/.

people based on their protected characteristics, including ethnicity, race and gender.[8] Even if this is not the stated aim of the technology, discriminatory impacts are nevertheless an inherent risk of this technology that can exacerbate and entrench existing societal disadvantages and further disempower already-marginalized groups of people.

Alongside the impact on the right to privacy, FRT also poses a direct threat to the enjoyment of the right to freedom of peaceful assembly and expression, among other rights. For example, law enforcement authorities have used facial recognition technologies to track down protestors, by using images captured through CCTV and other video surveillance devices and running them through facial recognition software to perform face analysis or search for potential face matches against a designated database.[9] Amnesty's research has shown that facial recognition-capable cameras are often casting a radius of exposure that covers up to 100% of sites of protest.[10]

FRT also undermines the right to equality and non-discrimination and can entrench and exacerbate existing inequalities, including through targeting protesters from marginalized communities.[11] Amnesty's research has shown that e.g. the New York Police Department's vast surveillance operation particularly affects people already targeted for racist stop-and-frisk policing, and that in three boroughs, the higher the proportion of non-white residents, the higher the concentration of facial recognition compatible CCTV cameras. While quite some attention has been paid to the global rise of real-time, or "live", facial recognition, retrospective facial recognition is far more pervasive, and uses existing older forms of video surveillance, such as CCTV, in combination with deeply problematic facial recognition software.

Further, in Hyderabad City, India, the government has initiated the construction of a "command and control centre" (CCC), connecting the city's vast CCTV infrastructure in real time.[12] The CCC supports the processing of data from up to 600,000 cameras at once. These cameras can be used in combination with Hyderabad police's existing facial recognition cameras to track and identify individuals across space. The construction of the CCC risks supercharging the already rampant rights-eroding surveillance regime, with no regulation in place to protect people.

Amnesty International and more than 200 organisations have called for an outright ban on uses of facial recognition and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance.[13]

In this regard, we recommend:

- That states ban the use, development, production, sale and export of facial recognition and remote biometric recognition technologies that enable mass surveillance and discriminatory targeted surveillance by state agencies and private sector actors.

DIGITAL REGULATION AND DATA PROTECTION

The surveillance-based business model of technology companies, in particular dominant 'gatekeeper' platforms such as Google and Facebook, represents an assault on the right to privacy on an unprecedented scale.[14]

It has become virtually impossible for users to engage in the digital world without being subject to ubiquitous corporate

[8] Ibid.

[9] Amnesty International, *Inside the NYPD's surveillance machine,* https://banthescan.amnesty.org/#stories.

[10] Ibid.

[11] Ibid.

[12] Amnesty International*, Ban the scan: Hyderabad*, https://banthescan.amnesty.org/hyderabad/.

[13] Amnesty International, *Amnesty International and more than 170 organisations call for a ban on biometric surveillance,* (7 June 2021), https://www.amnesty.org/en/latest/news/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/.

[14] Amnesty International, *Surveillance Giants: How the business model of Google and Facebook threatens human rights'* (21 November 2019), p. 5.

surveillance and intrusive profiling. Google and Facebook offer services to billions of people without asking them to pay a financial fee. Instead, citizens pay for the services with their intimate personal data. This data is used to analyse people, aggregate them into groups, and to make predictions about their interests, characteristics, and ultimately behaviour - primarily for advertising purposes. This represents an intrusion into billions of people's private lives that can never be necessary or proportionate. As with all systems of surveillance, this has disproportionate impacts on marginalised groups, and exacerbates existing structural inequalities.

Due to the interlocking and interdependent nature of human rights, this surveillance threatens a range of other rights beyond the right to privacy such as; freedom of expression and opinion, freedom of thought and the right to non-discrimination.

It is critical that states work together to enact and enforce strong digital regulation and data protection laws, that tackle surveillance-based business models in the tech sector.

In this regard we recommend that:

- States enact and enforce strong digital regulation and data protection laws, that overhaul surveillance-based business models in the technology sector, including by:
    - banning surveillance advertising that relies on invasive tracking and the processing of personal data
    - ensuring independent oversight over the algorithmic recommender systems used by online platforms and require them to be opt-in instead of an opt-out.
    - ensure people can practically choose rights-respecting alternatives to the dominant tech platforms.

- States should follow the recommendations of the UN Special Rapporteur on Freedom of Opinion and Expression including that:
    - "State regulation of social media should focus on enforcing transparency, due process rights for users and due diligence on human rights by companies, and on ensuring that the independence and remit of the regulators are clearly defined, guaranteed and limited by law."[15] [para 91]
    - The Special Rapporteur recognizes that "data protection is key to reorient the advertisement-driven business model of the digital economy". Amnesty International considers that this requires going further than "limiting pervasive tracking and targeting", and that States should ban surveillance advertising.
    - "In line with the Guiding Principles on Business and Human Rights, social media companies should review their business models and ensure that their business operations, data collection and data processing practices are compliant with international human rights standards."[16] [para 96]

ALGORITHMIC DECISION MAKING

The intrusive processing of personal data by Automated Decision Making (ADM) systems undermines the right to privacy. ADM can be used to analyse and predict certain personal aspects, such as performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

ADM system can be used in the public sector to filter and approve welfare payments, prioritise healthcare recipients and decide immigration applications, amongst other things.[17] Amnesty International's Xenophobic Machines report exposed how racial profiling was baked into the design of an algorithmic system used to determine whether claims for childcare benefit were flagged as incorrect and potentially fraudulent.[18] In these cases, individuals are often unaware that an

[15] OHCHR, *Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: Report on disinformation*, (13 April 2021), para 91.

[16] Ibid. Para 96.

[17] Amnesty International, *Xenophobic Machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal*, (25 October 2021) p. 5.

[18] Amnesty International, *Dutch childcare benefit scandal an urgent wake-up call to ban racist algorithms*, (25 October 2021) https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-

algorithm is being used and so are unable to consent to its use. Additionally, even when individuals know that these systems are in use, they often have no other equivalent way to apply for the services that they need, and so may consent out of necessity rather than choice. Such lack of meaningful consent can also be true when ADM systems are used in the private sector such as in job applications, for example.

Additionally, through the use of proxies, ADM systems can infer sensitive information about individuals based on limited shared information. From freely shared information, ADM systems build profiles about individuals which includes, potentially inaccurate, more sensitive and intrusive inferred information that has not been shared. This profiling of individuals demonstrates an intrusive processing of personal data and undermines the right to privacy.

Algorithms are also data-intensive technologies and therefore both accelerate data amassing trends in the public and private sectors, and can increase surveillance risks.

In this regard, we recommend that:

- States put in place a framework that
    - prevents human rights violations in relation to the use of algorithmic decision-making systems from taking place;
    - establishes monitoring and oversight mechanisms as safeguards;
    - holds those responsible for violations to account, and;
    - provides effective remedy to individuals and groups whose rights have been violated.
- Governments refrain from using black box and self-learning systems in high-risk contexts.
- Governments should a public registry of public sector use of these tools.

WEB3

The continued development of distributed ledger technologies – often referred to as "web3" – raises serious privacy concerns and potential violations of the right to privacy. Firstly, while blockchain and distributed ledger technology are theoretically pseudonymous, all transactions data on a "public" blockchain like Bitcoin or Ethereum is publicly available. As software engineer Molly White explains: "But if we think about this future world where all, or at least many more, transactions happen with cryptocurrencies, this has some serious ramification. Imagine if your entire credit card or Venmo history was publicly visible to anyone who wanted to go see it. And what if it's not just your one-off date who can see these transactions, but your ex-partner, or your estranged family member, or your stalker? What if your prospective employers could check out all of your financial transactions, and they could go back as far as they wanted?"[19]

Secondly, pseudonymity alone is not sufficient privacy protection. As US law firm Davis Polk explains, "Methods exist for linking individuals to public keys by analyzing blockchain transactions and other publicly available data. Some businesses offer services to identify individuals using their public keys, blockchain transactions, and other available data."[20]

Finally, web3 technology poses a challenge to some of the core tenants of data privacy laws including the General Data Protection Regulation (GDPR), which "perpetuate a traditional data protection framework" that assigns compliance responsibility to data controllers and processors.[21] According to Davis Polk, "blockchain technology's distributed peer-to-peer network architecture often places it at odds with the General Data Protection Regulation's (GDPR) and the California Consumer Privacy Act's (CCPA) traditional notion of centralized controller-based data processing. This disconnect can

scandal/#:~:text=The%20report%20Xenophobic%20Machines%20exposes%20how%20racial%20profiling,benefit%20were%20flagged%20as%20incorrect%20and%20potentially%20fraudulent.

[19] Molly White, *Abuse on the Blockchain*, (Stanford University Lecture: 7 March 2022), https://blog.mollywhite.net/abuse-on-the-blockchain-lecture/.

[20] Pritesh Shah, Daniel Forester, Matthias Berberich, Carolin Raspe, '*Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies*', Practical Law (2019), p. 4.

[21] Ibid. p.2.

make it difficult to reconcile current data protection laws with blockchain's other core elements, such as the lack of centralized control, immutability, and perpetual data storage."[22]

NEUROTECHNOLOGY

The continued development of neurotechnology poses huge privacy concerns. Today, brain-computer interfaces (BCIs) can read, in a limited way, what someone is thinking and can capture what someone is seeing by deciphering neurological signals without invasive procedures. State militaries, commercial enterprises and schools already monitor mental states, such as attention and fatigue. Further, technology already exists to enable individuals to communicate from human brain to human brain via the internet, for individuals to perform collective tasks through brain-to-brain communications and for consumers to control smart home devices, through non-invasive brain monitors, all at a rudimentary level.[23] The ultimate goal, for militaries, medical scientists, workplaces, and sellers of consumer goods, is to be able to read emotions and thoughts, implant emotions, knowledge and memories, and communicate directly between the brain and the internet or between people simply by thinking. Some researchers expect to be able to decode brain activity within 5 to 10 years.

The potential to read and implant thoughts, before thoughts are translated into any action, risks undermining the very foundation of personal identity and, within this, eliminating individual privacy. While some consumer wearables and home products can already read unconscious signals, such as micro-facial expressions, eye movements and speech modulation, and can attempt to influence actions based on those signals, reading thoughts directly is qualitatively different. Indeed, it would expose all of a person's identity, with nothing remaining hidden from the world. This would be particularly concerning in cases where an individual does not, or cannot, meaningfully consent.

The pervasive nature of neurotechnology also has potential to infringe on a broader range of human rights. Threats include: the undermining of autonomy and undue influence on opinions and choices; eliminating privacy; corporate and State surveillance; algorithmic bias; intentional discrimination based on the information obtained; discrimination on AI-identified characteristics and traits that have not historically been traits used to discriminate; unequal access to beneficial technologies; inadequate cyber security; and risks to other freedoms, such as freedom of association and freedom of speech.

OHCHR should develop clear recommendations for the application of existing human rights standards in the context of such potentially invasive new technology, before the practices are widely adopted. This includes clear accountability safeguards for both states and corporate actors.

ENCRYPTION AND ANONYMITY

Encryption protects people's human rights online. By rendering digital data unintelligible, encryption helps ensure that private information sent over the internet stays private. It also allows people to access safe online spaces where they can speak freely and express their ideas and opinions.

The General Assembly, UN Special Procedures, and human rights groups recognise that encryption is a vital enabler of human rights, in particular for the rights to privacy and to freedom of expression and opinion. Access to encryption may also have an impact on other rights such as the right to peaceful assembly and association.

The report should highlight agreed language from UNGA resolution 75/176 recognising the importance of encryption and anonymity tools.

In this regard we recommend:

[22] Ibid. p.3.

[23] Erin Biba, *Brain-to-Brain communication is closer than you think*, (7 June 2016), http://popularmechanics.com/science/a21220/brain-brain-communication., Robert Martone, *Scientists demonstrate direct brain-brain communication in humans*, (29 October 2019), http://scientificamerican.com/article/scientists-demonstrate-direct-brain-to-brain-communication-in-humans.

- Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption, pseudonymization and anonymity, are important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of opinion and expression and to freedom of peaceful assembly and association. States should refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking.
- Business enterprises should work towards enabling technical solutions to secure and protect the confidentiality of digital communications.
- States should not interfere with the use of such technical solutions, with any restrictions thereon complying with the obligations of States under international human rights law, and enact policies that recognize and protect the privacy of individuals' digital communications.