AMNESTY INTERNATIONAL

TOWARDS A GLOBAL MORATORIUM ON TARGETED SURVEILLANCE TECHNOLOGY

INTRODUCTION

Digital attacks against human rights defenders, journalists and civil society are on the rise. There is mounting evidence of human rights violations being committed by governments and companies from unlawful targeted surveillance of activists, journalists, lawyers and others. Too many states around the world have so far turned a blind eye and allowed the export of surveillance technology to governments that have a track record of using spyware to violate human rights. These violations can no longer be ignored.

The idea for a surveillance exports moratorium was first given global prominence by then UN Special Rapporteur on Freedom of Expression David Kaye, who in his 2019 report recommended that "States should impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place."[1] Since then, this call has been taken up by states,[2] human rights experts[3] and numerous civil society actors.

WHAT IS UNLAWFUL TARGETED SURVEILLANCE?

Unlawful targeted surveillance has two key dimensions. The first arises when people are targeted for surveillance based on their exercise of their human rights, or due to their identity in a discriminatory fashion. There are numerous examples of such cases, wherein journalists are targeted for their reporting on issues critical of a government, where activists are targeted for organizing protests, or where people of a certain ethnicity, race, sexual orientation, religion, etc. are targeted on a discriminatory basis as criminals or potential criminals.

Targeting people for surveillance on such bases is never in accordance with human rights law.

The second dimension of unlawful targeted surveillance includes cases where targeting may have some legitimate basis – such as where an individual is reasonably suspected of criminal wrongdoing – but the system that allows such surveillance may itself be unlawful where it does not provide adequate safeguards (including remedies) against abuse.

Amongst the most important reasons why this is so has to do with the concept of "chilling effects". In this context, 'chilling effects' refers to the phenomenon whereby people refrain from exercising their rights out of fear they could be subject to surveillance. In other words, "Even the mere possibility of communications being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association."[4]

Research bears out that activists who fear – even without proof – that they are under surveillance will be less likely to be willing to speak out critically of the government, to organize protests, to meet freely with colleagues, or even to speak on the phone or send emails, not knowing how such activities could later be used against them.[5]

Such self-censorship arises when states fail to enact adequate safeguards, so that it may be impossible to know who is

---

[1] Report of the Special Rapporteur, David Kaye, A/HRC/41/35 (2019), p. 20.

[2] https://www.accessnow.org/costa-rica-first-country-moratorium-spyware/

[3] "Spyware Scandal: UN experts call for moratorium on sale of 'life-threatening' surveillance tech," 12 August 2021, https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening?LangID=E&NewsID=27379

[4] UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, A/HRC/27/37, 30 June 2014 (hereinafter UNHCHR Privacy in the Digital Age), para. 20.

[5] Amnesty International, Belarus: "*It's enough for people to feel it exists" : Civil society, secrecy and surveillance in Belarus* EUR 49/4306/2016, https://www.amnesty.org/en/documents/eur49/4306/2016/en/?msclkid=a728523ac7b611ec83ec6bce36b64552

subject to surveillance, how, or why. In such cases, "widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified […]. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right [to private and family life]."[6]

In other words, where safeguards are inadequate, it is not just the rights of individual targets who are affected, but the rights of everyone.

A MORATORIUM AS A STRENGTHENING OF RIGHTS

While research by civil society and media organizations has demonstrated that both types of unlawful targeting exists on a massive scale, it is also clear that unlawful targeted surveillance due to lack of safeguards is nearly universal. As former Special Rapporteur David Kaye summarized it "It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broke. It hardly exists."[7] Without an immediate moratorium, the unlawful use of surveillance technology will continue to have devastating effects on the human rights not only of targets, but of everyone.

A moratorium on spyware serves two main goals – 1) to halt the sale, transfer and use of spyware, but crucially also 2) to strengthen human rights safeguards.

In light of this, perhaps the most apt way of conceiving of a moratorium is the strengthening of the right to privacy (and other associated rights impacted by unlawful surveillance.) In effect, a moratorium is a restating of the existing prohibition against unlawful surveillance, and a strengthening of human rights.

POSSIBLE MODELS

A spyware moratorium would have to take the form of a list of human rights safeguards states would be required to put in practice in order to be authorized to carry out the sale, transfer or use of targeted surveillance technology.

International human rights law provides numerous examples of how this could be achieved. For example, the Arms Trade Treaty, [8] or the proposed treaties to regulate lethal autonomous weapons systems (so-called "killer robots"),[9] or the trade in "tools of torture" [10] all provide criteria whereby states must enact safeguards around tools or technology capable of both legitimate and illegitimate uses in order to ensure against abuses resulting from their manufacture, use or transfer.

CONCLUSION

The case for the necessity of a global moratorium on the sale, transfer and use of targeted surveillance technology is clear and urgent. The unregulated and untransparent sale and use of these products means that we may never know the full extent of similar abuses involving other actors. The world can no longer turn a blind eye to this enormous global threat to our rights.

Comments or questions? Contact: rebecca.white@amnesty.org

---

[6] Roman Zakharov v. Russia, European Court of Human Rights, paragraph 171.

[7] Report of the Special Rapporteur, David Kaye, A/HRC/41/35 (2019), p. 46.

[8] Arms Trade Treaty, adopted April 2, 2013, A/RES/ 67/234B, entered into force December 14, 2014, art. 7.

[9] Human Rights Watch, *New Weapons, Proven Precedent: Elements of and Models for a Treaty on Killer Robots*, October 2020, https://www.hrw.org/report/2020/10/20/new-weapons-proven-precedent/elements-and-models-treaty-killer-robots

[10] Amnesty International, *Ending the Torture Trade: The Path to Global Controls on the 'Tools of Torture'* https://www.amnesty.org/en/wp-content/uploads/2021/05/ACT3033632020ENGLISH.pdf?msclkid=767b8160c4aa11ec95b9bedfcb8839f1