Civic Space & Tech Brief

Hacking & Spyware

Hacking is a type of **covert interference with digital devices**, such as laptops and mobile phones, that enables access to personal and confidential information without authorization by, or knowledge of, the user(s), owner, or manufacturer. While it can be legal, it is often done for **unlawful surveillance purposes**, using spyware tools. While no robust data is available, **incidents of state and state-affiliated actors using spyware seem to be on the rise**.

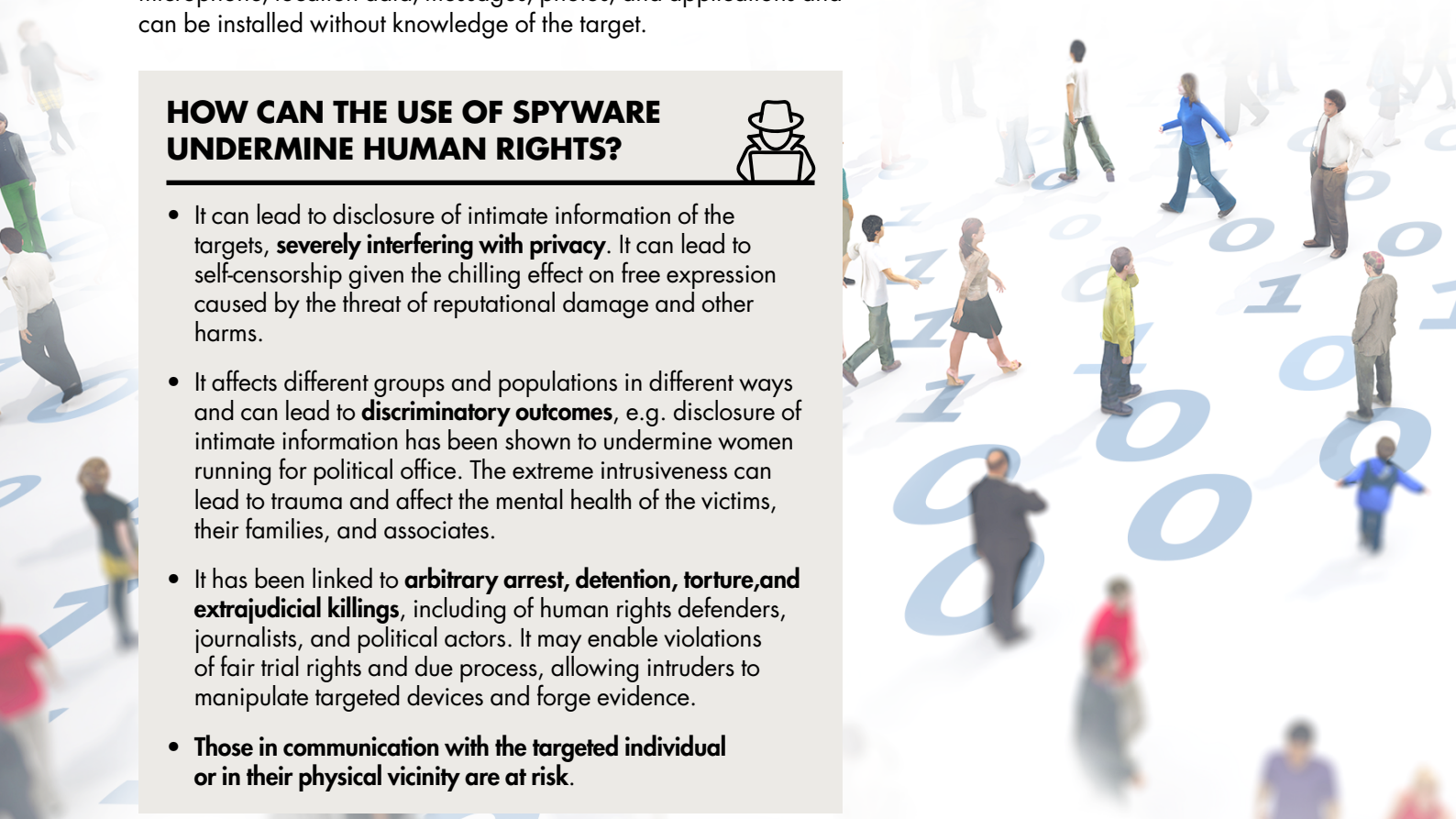
Hacking for surveillance purposes allows the intruder to **obtain details about the target's opinions, activities, health, and other potentially sensitive information**. Spyware tools can be used to switch on devices' cameras and microphones or delete and otherwise manipulate stored data.

Highly invasive spyware is widely available on the global market. Spyware tools provide authorities and others with far-reaching powers to invade people's privacy and access confidential data. They can be used to obtain access to all parts of a device, including camera, microphone, location data, messages, photos, and applications and can be installed without knowledge of the target.

> *While purportedly being deployed for combating terrorism and crime, spyware tools have often been used for illegitimate reasons, including to clamp down on critical or dissenting views and on those who express them, including journalists, opposition political figures and human rights defenders.*
>
> *HC report on the right to privacy in the digital age (A/HRC/51/17, 2022)*

HOW CAN THE USE OF SPYWARE UNDERMINE HUMAN RIGHTS?

- It can lead to disclosure of intimate information of the targets, **severely interfering with privacy**. It can lead to self-censorship given the chilling effect on free expression caused by the threat of reputational damage and other harms.
- It affects different groups and populations in different ways and can lead to **discriminatory outcomes**, e.g. disclosure of intimate information has been shown to undermine women running for political office. The extreme intrusiveness can lead to trauma and affect the mental health of the victims, their families, and associates.
- It has been linked to **arbitrary arrest, detention, torture,and extrajudicial killings**, including of human rights defenders, journalists, and political actors. It may enable violations of fair trial rights and due process, allowing intruders to manipulate targeted devices and forge evidence.
- **Those in communication with the targeted individual or in their physical vicinity are at risk**.



STAND UP FOR HUMAN RIGHTS
#STANDUP4HUMANRIGHTS

UNITED NATIONS HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Civic Space & Tech Brief

STAND UP FOR HUMAN RIGHTS
#STANDUP4HUMANRIGHTS

UNITED NATIONS HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

> *Noting with deep concern […] the use of technological tools developed by the private surveillance industry […], hacking of devices and systems, interception and disruption of communications, and data collection, interfering with the professional and private lives of individuals, including those engaged in the promotion and defence of human rights and fundamental freedoms, journalists and other media workers, in violation or abuse of their human rights, specifically the right to privacy.*
>
> *GA Resolution on the right to privacy in the digital age (A/RES/77/211, 2022)*

The UN and numerous regional organisations have recognized that the intrusive and indiscriminate nature of spyware tools pose unique and grave threats to privacy and other human rights. Human rights law thus requires States to ensure that:

- ✓ Any State hacking must be legally authorised by independent courts and meet the requirements of international human rights law, namely be **based on law, pursue a legitimate aim, be necessary, and proportionate** and in accordance with the principle of non-discrimination.
- ✓ The **essence of the right to privacy is not undermined**.

KEY MEASURES TO END ABUSES:

STATES SHOULD

- **Limit the availability of intrusive surveillance technology** through a moratorium on the sale, transfer and use of hacking tools until human rights compliance can be ensured;
- **Include the right to privacy in legislation** and ensure that national law strictly regulates the use of hacking and introduce safeguards to secure the confidentiality of users;
- **Promote and protect** end to end encryption and legislate against client-side scanning;
- **Use hacking only as last resort,** subject to prior approval by a judicial body and rigorous independent oversight and limit use to prevent or investigate specific acts that constitute serious threats to national security or serious crimes, and narrowly targeted at the person suspected of committing those acts. Be clear which authorities can use hacking and transparent who does and limit access to data to those necessary to respond to the threat at hand;
- Conduct **regular and comprehensive human rights impact assessments** and systematically assess potential risks and damage to the security and integrity of the targeted device, as well as the data.

BUSINESS ENTERPRISES PROVIDING SURVEILLANCE TOOLS SHOULD

- **Conduct human rights due diligence** and ensure accountability and the provision of remedies, in accordance with the UN Guiding Principles on Business and Human Rights;
- **Refrain from selling spyware to states that have a record of unlawful surveillance;**
- **Put in place escalation procedures** when there is a risk of violent conflict.

For more details, see our report A/HRC/51/17 on the right to privacy in the digital age.