Factsheet: Spyware and Digital Surveillance

Background

In the world of advanced methods of data collection, graphics processing and algorithms, there is wide-spread concern that the increasing prevalence of spyware and digital surveillance pose a serious threat to human rights, most notably, privacy and freedom of expression.

Spyware and surveillance may take various forms, including but not limited to electronic trackers, security and monitoring systems, apps, data disclosure by companies, malware etc. For many, the knowledge of being surveilled — or even of the risk of potentially being surveilled — may lead to self-censorship. Additionally, the risk of data misuse, theft and breaches are legitimate and worrisome aspects of surveillance.

A number of domestic and international bodies have developed principles and safeguards to be applied in the event of surveillance, particularly on a mass scale, and the use of interception technologies. These principles, together with other surveillance considerations, are discussed below.

Biometric data and facial recognition technology

Article 4(14) of the General Data Protection Regulation of the European Union (GDPR) defines 'biometric data' as "personal data resulting from specific technical processing relating to the physical, physiological or behaviour characteristics of a natural person, which allow the unique identification of that natural person, such as facial images or dactyloscopic data." One form of biometric data is facial recognition technology (FRT), which makes use of photos and/or videos to capture the geometry and features of a natural person's face and to create a "faceprint". This faceprint may then be stored by the software in use. FRT also commonly extends to the recording of fingerprints.

One of the most glaring issues with biometric data and FRT is that it may regularly misidentify people based on demographical details such as age, race or gender. A recent study conducted by the National Institute of Standards and Technology confirmed that facial-recognition technology was 100 times more likely to misidentify people of colour than white people, and women, the elderly and children were also misidentified at a higher rate.

More broadly, FRT may implicate a broad array of rights beyond just the right to privacy. For example, freedom of association may be implicated if people are recorded gathering, which in turn has consequences for freedom of expression. Likewise, freedom of movement can be at risk. The Article 29 Working Party stated in their 2004 Opinion on the processing of personal data by means of video surveillance that Article 2 of Additional Protocol No. 4 to the European Convention for the Protection of Human Rights and Fundamental Freedoms protects the right to free movement of individuals, who have "the right to exercise their freedom of movement without undergoing excessive psychological conditioning as regards their movement and conduct as well as without being the subject of detailed monitoring such as to allow tracking their movement and/or triggering "alarms" based on software that automatically "interprets" an individual's supposedly suspicious conduct without any human intervention — on account of the disproportionate application of video surveillance by several entities in a number of public and/or publicly accessible premises."

In this way, FRT and video surveillance technologies may also have consequences for the right to equality and non-discrimination, and the right to dignity. 'Suspicious activity' is usually

poorly and vaguely defined and oversight mechanisms often do not exist to enable auditing of the criteria by which such behaviour is identified. As has been argued in a court case regarding video surveillance technology in South Africa, "even where discrimination is not intended, indirect discrimination can result from using innocuous and genuinely relevant criteria that also operate as proxies for race and ethnicity."

Finally, video surveillance systems may also infringe on the rights of children who pass through their spheres of data collection by indiscriminately collecting personal information about them.

Although there is potential for these rights to be infringed by FRT and video surveillance technology, it is not inevitable that the right to privacy and the interested of security should be opposed. Security can certainly be pursued if appropriate precautions are taken.

Surveillance safeguards

There are ten widely recognized principles to limit the harm which may be caused by surveillance regimes, including those implemented by government. These principles provide a framework which aims to uphold fundamental rights and, ideally, are to be read together with domestic legislation that would sufficiently restrict digital interception. The principles are summarised below:

- Legality: there must be a sufficiently clear and accessible legal framework to enable interference. Legislation should align with international standard and must be periodically reviewed.
- Security and integrity of systems: the state should, prior to proceeding with interference and hacking, assess the integrity of the security systems in question. In the event of data breaches or compromises, there should be practical mitigation techniques.
- Necessity and proportionality: according to standard guidelines under international law for restricting the right to freedom of expression, surveillance and hacking should be necessary and proportionate in a democratic society. This means the measures taken should be necessary to achieve a legitimate purpose, and the powers authorising a means of surveillance should be narrowly defined. The interfering party, generally the state, should demonstrate that there are no alternative measures to meet the purpose, and that the response is proportionate to the security risk faced. When security measures may implicate human rights, they should contain appropriate safeguards to protect against the unjustifiable infringement of rights, examples of which are elaborated on further in this list.
- Judicial authorisation: state authorities must make application to a competent and independent judicial authority, regarding the measures which will be taken to implement surveillance.
- Integrity of information: interfering parties ought not to compromise or alter any data collection.
- Notification: persons who are surveilled must be made aware of this. In the event that the state or a third party seeks personal data from service providers, these providers should notify users.
- Destruction and return of data: any additional data and information which is not needed must be properly destroyed or returned. Moreover, pursuant to the fulfilment of the legitimate purpose, data which is recorded should not be retained for longer than necessary.
- Oversight and transparency: the state must be transparent and accountable about the extent of its interference mechanisms and powers.

- Extraterritoriality: transparency is essential where the state is collecting data outside of the bounds of its territory. In this regard, government must comply with mutual treaties, if these are in place, and generally, with international human rights standards.
- Effective remedy: persons who are subject to unlawful interference must be granted access to effective remedies to challenge this.

The aforementioned principles have been published by numerous groups and in some circumstances, they have extended into further principles. A comprehensive source of reference is ARTICLE 19's report 'Global Principles on Protection of Freedom of Expression and Privacy: A policy brief.'

Tips for general digital security

Journalists, lawyers, activists and others who are at heightened risk of surveillance should take care to implement basic digital security practices that can protect against the unwanted intrusion on private communications. Some suggested guidelines include:

- Be mindful and selective of the information which you voluntarily share online.
- Do not visit insecure websites.
- To the extent possible, communicate through encrypted channels.
- Use strong passwords on your electronic devices, and be intentional about not using the same password for more than one account. Frequently update your passwords.
- Disable your location services, where possible.

Further resources:

The European Union General Data Protection Regulation 2016/679 may be accessed here.

The United Nation has published a 'Resolution on the Right to Privacy in the Digital Age', which may be accessed here.

For information on anonymity and encryption, see 'Report on anonymity, encryption and the human right framework,' which may be accessed here.