FACTSHEET #5
SECURITY AND DATA PRIVACY

WHY DO YOU NEED TO KNOW ABOUT SECURITY AND DATA PRIVACY?

In recent years, governments worldwide have tightened **security measures** by collecting more personal data. This, together with advancing technical possibilities to collect and analyse data, is eliminating our last remaining 'islands' of privacy. The need for a **trade-off between security and privacy** dominates public debates and political decision-making - but rather than focus on the root causes of insecurity (e.g. crime, terrorism), the preferred strategies are often those for which ICTs provide 'answers'. This factsheet explains the changing relationship between security and data privacy.

KEY MESSAGES

- Growing public acceptance of **surveillance technologies**, and the dramatically increasing capabilities of these, threatens the essence of our right to privacy.
- As more data is collected for security reasons, there is a risk of more **intrusions into human rights** without any actual security gains - or even of this leading to adverse security outcomes.
- A **proportionality principle** would require that, when gathering personal data for security reasons, governments (and others) should always choose the least intrusive option.
- **Public security objectives** form the basis of one of the exemptions from the GDPR's strict regulations on the use of personal data (Article 2, paragraph 2d).

VULNERABLE PEOPLE AND SECURITY

There has been a shift in recent decades towards predictive policing – the use of analytical techniques to **identify potential criminal activity before it happens**. This raises ethical concerns, though: by relying on predictive technologies, police officers could see certain people in society as 'likely' to be involved in crime, and treat them as offenders - but this violates the 'presumption of innocence' principle. Predictive policing is based on historical data, meaning its conclusions assume that the future will reproduce the past - which can lead to bias and prejudice.

HOW NATIONAL SECURITY CAN INFRINGE PERSONAL RIGHTS

Being flagged as 'potentially dangerous' by an automated national security system can have serious consequences. Because the decision-making process of Artificial

Intelligence (AI) algorithms is usually based on complex mathematical functions (see factsheet #3), it can be hard or impossible to obtain an understandable explanation for the results. This is important, since **the right to data access is often limited in the context of national security**, and such data is treated as confidential. For the person affected, it may, as a result, be difficult to find out why they are subjected to certain measures, such as frequent checks at airports.

WHAT YOU CAN DO

- Through encryption, you can prevent data on your computer's hard drive from being accessed by external subjects; also, consider encrypted email services to exchange sensitive content, or encrypted services for private messages (e.g. Signal).
- Practice 'data protection hygiene' - for example, do not share sensitive personal data, and avoid using cloud services to share sensitive documents.
- Use strong passwords to protect your accounts - and don't reuse the same password on different services.
- Check Electronic Frontier Foundation's Surveillance Self-Defense website for more on these strategies: bit.ly/3wQ3PfB

FIND OUT MORE

READ: This factsheet is based on PANELFIT's 'Issues and gaps analysis on security and cybersecurity', which you can read here (bit.ly/3vQm5Ej, PDF). Privacy International's 'Secure safe spaces online' offers information and practical advice on encryption, online anonymity and human rights (bit.ly/3d6v11l, PDF). You should also read the PANELFIT factsheets on AI (#3) and data privacy (#4).

WATCH / LISTEN: Two PANELFIT monthly chats discuss how surveillance policies affect national and societal security (bit.ly/3d5CzSt) and the issues and gaps analysis on security and cybersecurity (bit.ly/35NtUjw). The *Citizenfour* documentary by Laura Poitras also covers these subjects (bit.ly/35J2qve).