Global policy recommendations and action framework on the surveillance of journalists

Principles

- The surveillance of journalists constitutes an attack on media freedom, the protection of sources and the public's right to information
- It also represents a risk to health and safety at work
- When it targets trade union activities, it undermines freedom of association and trade union rights
- Digital safety is a collective responsibility that rests primarily with states, employers and technology companies.
- Media employers, journalists' unions, media support organisations and individual journalists all have a shared responsibility to protect and improve the working environment from the threats posed by surveillance
- The surveillance industry, technology and AI companies, internet and telecommunication providers and states must carry the financial burden of the costs of prevention measures and reducing the harm inflicted on journalists and the media as a result of the threat or use of surveillance.

- Freelance and self-employed journalists must enjoy the same level of protection against surveillance as staff journalists, including access to preventive measures, secure equipment, training, technical and legal assistance, and effective remedies, regardless of their employment status.

Commitments by trade unions and media organizations

- Adopt a global policy and action plan
- Establish a secure platform for the reporting of surveillance incidents and a rapid response mechanism
- Appoint regional focal points
- Develop, in collaboration with media specialist partners, a network of regional forensic capabilities
- Provide technical, legal, trade union and psychological support
- Document attacks and identify their transnational dimensions
- Integrate digital monitoring into the IFJ's general safety programmes
- Support affiliates in negotiating collective safeguards
- Collaborate with scholars to further research on surveillance and its impacts
- Publish an annual report on implementation.

States' obligations and international responsibility

- A presumption that the surveillance of journalists and their sources is prohibited
- An absolute ban on any surveillance motivated by journalistic or trade union activity
- A moratorium on the sale and export of intrusive spyware to countries that lack clear regulation and legal restriction against using it to monitor journalists
- A ban on mass surveillance and blanket data retention
- Strict regulation of any exceptional measures, subject to prior judicial authorisation which should include specification of what surveillance tools can be used and by whom
- The abolition of general exemptions relating to national security or states of emergency
- Enhanced protection for sources, including the prohibition of the use of metadata to try to identify them.
- Transparency in public procurement of surveillance technologies.
- Subsequent notification of individuals subject to surveillance;
- Independent investigations, effective remedies, compensation and sanctions
- Legal and technological restrictions on using AI hacking capabilities on journalists and trade union and human rights activists.
- Legal restrictions on the collection and commercial sale of personal data harvested by technology companies that can identify personal details and activities of journalists and human rights defenders.

Media employers' duty of care

- Risk assessments to be carried out prior to sensitive assignments and investigations
- The provision, free of charge, of secure equipment and communications tools
- Ongoing digital security and safety training during working hours
- The preservation of evidence of surveillance and the use of independent expertise to verify attacks
- Legal, technical and psychological support to be provided to journalists affected
- The safeguarding of employment, pay and assignments whilst an incident is being dealt with
- Equal protection for employees, freelancers, self-employed workers, local correspondents, fixers and technicians
- Mandatory consultation with trade unions when drawing up security policies.

Obligation of Due Diligence

The obligation of Due Diligence is enshrined in international law. While currently there is no specific international agreement or standards regulating the sale and use of surveillance technologies, existing Due Diligence guidelines adopted by the UN, OECD and the EU allows the UN and/or other regional intergovernmental organizations to establish a

mechanism to monitor and report on the commitment of states and the private sector to their obligations. The IFJ will work with its affiliates, international trade union movement, human rights and freedom of expression organisations and consult with international and regional mandate holders to advocate for establishing such a mechanism. The mechanism will in particular monitor and report on the actions of:

States:

- To establish domestic legal frameworks that compel tech firms to build human rights safeguards directly into their product architectures
- To ensure that state intelligence and law enforcement agencies only procure tools from developers with verifiable human rights compliance records, and use them in accordance with international human rights standards
- To establish an export registry and deny export licenses if there is a real risk the tech will be used for internal repression or human rights abuses

The private sector:

- To build technical constraints into the software to limit illegal or unauthorised use
- To map the end-user's human rights record and legal tracking history
- To require clients importing surveillance technology and/or software to sign terms that explicitly forbid targeting journalists, activists or dissidents.

Cooperation with trade unions, media, experts and partner organisations

- Promoting cooperation and joint actions to expose and address threats posed by surveillance with organisations defending press freedom and human rights
- Establishing secure networks for sharing alerts
- Carrying out joint investigations into sellers and user states;
- Undertaking strategic litigation at national and international level;
- Organising the training of local specialists;
- Launching joint public campaigns to expose and combat surveillance;
- Providing support for direct and indirect victims: sources, colleagues, relatives and trade union representatives.