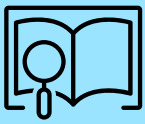
Recommendations for PRIVACY REGULATORS

1 **Establish Clear Definitions and Regulations for Stalkerware**

Create precise and comprehensive definitions of stalkerware within privacy regulations to ensure effective identification and appropriate handling of these apps.



2 **Engage with App Stores and Device Manufacturers**

Collaborate closely with app stores and device manufacturers to identify and remove stalkerware apps and features from their platforms and devices.

3 **Conduct Audits and Investigations in Collaboration with Technology Companies**

Regularly audit and investigate app stores to identify apps exhibiting stalkerware behavior and address any privacy violations. Additionally, conduct regular audits of anti-stalkerware solutions and IPV-victim support websites.

4 **Implement Effective Reporting Mechanisms**

Create accessible channels for reporting stalkerware incidents to law enforcement and relevant authorities for prompt and appropriate action.

5 **Enforce Strict Penalties**

Ensure severe penalties are imposed on individuals or entities involved in the development, distribution, or use of stalkerware for malicious purposes.

6 **Raise Awareness through Education Campaigns**

Launch public awareness initiatives to educate individuals about the risks of stalkerware and empower them to detect and protect against such intrusive apps.

7 **Facilitate International Cooperation**

Encourage collaboration among countries to tackle cross-border challenges related to stalkerware due to its potential use across various jurisdictions.

8 **Support Research and Innovation**

Allocate resources to support research and innovation in the field of privacy and security specifically related to IPV and stalkerware.

This project was funded by

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Concordia University

For more information, scan this QR code