RESOLUTION ON SOCIAL MEDIA AND VIOLENT EXTREMIST CONTENT ONLINE

41st International Conference of Data Protection and Privacy Commissioners

22 October 2019, Tirana, Albania

***SPONSOR*:**

- Office of the Privacy Commissioner, New Zealand

CO-SPONSORS:

- Office of the Australian Information Commissioner
- Office of the Privacy Commissioner of Canada
- Data Protection Commissioner, Council of Europe
- Data Protection Ombudsman, Finland
- Commissioner for Data Protection and the Freedom of Information Rhineland-Palatinate, Germany
- Privacy Commissioner for Personal Data, Hong Kong, China
- Information Commissioner, Jersey
- Data Protection Authority, Luxembourg
- Information and Data Protection Commissioner, Malta
- National Privacy Commission, Philippines
- National Personal Data Authority, Tunisia
- Information Commissioner's Office, United Kingdom

The 41st International Conference of Data Protection and Privacy Commissioners:

Recalling that the 30th International Conference of Data Protection and Privacy Commissioners resolved to identify the need for data and privacy protection in social network services[1];

Noting that social media services have evolved to be more pervasive, with wider usage and newer technologies such as livestreaming;

Recognising that social media providers have a responsibility to consider the privacy and human rights impact of their content policies;

Noting that social media providers may have significantly different content policies and different rules about what kinds of content can be removed;

Recognising that the use of social media to distribute images, videos or other content of victims of terrorist violence has adverse impacts on the privacy and human rights of the victims, on collective security and on people throughout the world;

Recognising that social media services have been used to spread terrorist content since such platforms are easily accessible by all;

Concerned that terrorist attacks in recent years, such as in Christchurch in March 2019, have abused the services of social media providers through disseminating terrorist or violent extremist content online;

Concerned that personal data are used to identify targets for radicalisation to extremist views and that social media collects different types of personal data that act as an enabler to identify such targets;

Noting that terrorist and violent extremist content has several harmful impacts on individuals, communities and society as a whole;

Recognising that social media providers have a great responsibility to protect their users from the harms of terrorist and violent extremist content available on their platforms;

Noting the Christchurch Call for collective action between governments and online service providers to combat the dissemination of terrorist and violent extremist content online[2];

Recognising the significant steps already taken to address this issue by bodies such as the EU Internet Forum; the G20, and the G7 (including work underway during France's G7 Presidency on combating the use of the internet for terrorist and violent extremist purposes); the Global Internet Forum to Counter Terrorism (GIFCT); the Global Counterterrorism Forum; Tech Against Terrorism; and the Aqaba Process established by the Hashemite Kingdom of Jordan.

[1] ICDPPC Resolution on Privacy Protection in Social Network Services https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-Protection-in-Social-Network-Services.pdf
[2] Christchurch call to action to eliminate terrorist and violent extremist content online https://www.christchurchcall.com/

Therefore the 41st International Conference of Data Protection and Privacy Commissioners resolves to:

a. Urge social media providers to protect their services and users data from misuse and to stop the dissemination of terrorist and violent extremist content online while protecting freedom of expression;
b. Urge social media providers to continue to protect freedom of expression while trying to identify and classify published content as terrorist and violent extremist content to counter terrorist and violent extremist content online;
c. Encourage social media providers to inform relevant law enforcement agencies of terrorist and violent extremist content published on their platforms and the steps taken to delete the content, in a manner consistent with the rule of law and human rights protections;
d. Urge social media providers to publish clear policies that identify the types of content that would amount to terrorist, violent extremist and unlawful content ensuring social media users are aware of the types of content that will be removed and deleted;
e. Urge social media providers to be accountable for the content they remove to ensure protections of freedom of expression;
f. Encourage social media providers to recognise the potential for user data to be used to target violent extremist content, and to create tools to detect and delete violent extremist content published on their platforms, in a manner consistent with the rule of law and human rights protections;
g. Urge social media providers to change their content polices to ensure that terrorist or violent extremist content is listed, in a transparent manner, as unlawful content that breaches the rights and freedoms of the individuals depicted in such content, as well as the interests of the wider community, including those related to national security, public safety, and prevention of disorder or crime;
h. Encourage the development of industry standards to prohibit the dissemination of terrorist, extremist content and other violent unlawful content;
i. Encourage governments to ensure effective enforcement of applicable laws that prohibit the production or dissemination of terrorist and violent extremist content online, in a manner consistent with the rule of law, due process and international human rights law, including freedom of expression and data protection;
j. Urge governments to establish a legislative framework for cross border cooperation between national regulatory authorities to take down terrorist and violent extremism content in a timely manner; and
k. Urge collaboration between governments, social media providers and relevant civil society organisations, media and other key stakeholders to identify and to control the dissemination of terrorist and violent extremist content online.

EXPLANATORY NOTE

The internet is not immune from abuse by terrorist and violent extremist actors. This was tragically highlighted by the terrorist attacks of 15 March 2019 on the Muslim community of Christchurch – terrorist attacks that were designed to go viral. The dissemination of such content online has adverse impacts on the human rights of the victims, on our collective security and on people all over the world[3].

The Conference resolution seeks to start to build on the existing work specifically in the context of privacy and data protection.

The resolution highlights the roles of various stakeholders and institutions. It emphasises the responsibilities of business and governments to respect privacy and human rights.

The U.S. Federal Trade Commission abstains from this resolution, which relates to matters outside its jurisdiction.

The Argentina National Direction for Personal Data Protection, European Data Protection Supervisor, Italy Data Protection Commission, Portugal National Data Protection Commission and Switzerland Federal Data Protection Commissioner also abstain from this resolution.

[3] Christchurch call to action https://www.christchurchcall.com/call.html