While summarising the state of these discussions around ethics and privacy, this GNET report identifies the limits of and opportunities for research and formulates related recommendations for researchers and tech companies.

The nexus between terrorism and technology is socially and politically more relevant than ever. Almost every mobilisation and radicalisation process and every violent attack, whether carried out or prevented, has an online component to it.

Even when taking into account ever changing platforms and policies, as well as the shift towards ever more closed and encrypted spaces, there is abundant empirical data.

This abundance creates challenges and opportunities of its own, yet there are also hard limits to and grey zones around what a researcher dealing with extremist online content can and is allowed to do, which brings in ethical and data protection considerations.

Discussions of such topics gained much relevance in recent years and are particularly lively in international research consortia.

The most important findings are:

- More cross-platform access points and databases would provide incentives for a broader and more vibrant research field.
- Adly needed international research collaboration around analysing extremist online content would benefit from greater international harmonisation and a convergence of data protection rules.
- The dynamic empirical field requires regular mechanisms of exchange between tech companies, researchers and regulators to adapt policies, habits and legal frameworks in a way that does justice to the social and political relevance of the nexus between extremism and technology.
- Data protection regimes should not be seen as inconveniences but as enabling research by providing a clearer demarcation of what is and is not possible.

You can download this report and all our other publications for free at www.gnet-research.org