



GIFCT

Global Internet Forum
to Counter Terrorism

GIFCT Legal Frameworks Working Group

July 2021



GIFCT

Global Internet Forum
to Counter Terrorism

Policy issues and concerns arising from the legal frameworks regulating data have been identified by numerous stakeholders as being increasingly important as the technology industry has expanded its collaboration and proactivity around terrorist and violent extremist content (TVEC).

The Global Internet Forum to Counter Terrorism (GIFCT) Legal Frameworks Working Group brought together a range of different stakeholders, including Government, civil society, technology companies, academics, regulators and practitioners. This paper is intended to capture the range of discussion topics covered by the group, outline the primary issues the group identified, and highlight potential areas for further work and discussion.

None of the statements or opinions expressed in this paper are intended to represent the position of any individual or organization involved, nor of GIFCT itself.

Introduction

Legal frameworks intersect in a number of ways with efforts to disrupt terrorist and violent extremist use of the internet. Legal frameworks, whether in relation to data protection or privacy laws, can provide important clarity and structure to these efforts, but they can also lead, often through a lack of clarity, to adoption of corporate policies that limit the potential for multi-stakeholder collaboration and impact. These implications may not have been intended by policymakers. At the same time, this lack of clarity is compounded by a complex geopolitical landscape, contrasting national legal approaches to terrorism, a lack of global alignment on content standards, and the growing breadth of platform regulation can undermine efforts to craft clear legal frameworks, which enable and encourage impactful identification and mitigation of risks, including through data sharing, while protecting human rights. By contrast, these trends can instead lead to cautious, risk-averse approaches which broadly prohibit or limit data retention and sharing without considering a rights-balancing approach. More broadly, the issue of how these legal frameworks impact potential evidence of grave international crimes is one that requires urgent consideration.

Scope

In the context of terrorist and violent extremist use of the Internet, the most commonly discussed legal frameworks relate to the designation of terrorist organizations. Many countries establish domestic, and potentially multilateral, legal frameworks for this purpose, in addition to international efforts under the UN umbrella. The myriad range of challenges and long standing political complexities of these frameworks has been discussed in a number of forums already and remains the subject of legal and academic review.

As such, for its first paper, the GIFCT Legal Frameworks Working Group chose to focus on the issues relating to the work of technology companies disrupting terrorist and violent extremist content (TVEC) and the intersection with access to data. This was based on a discussion at the 2019 GIFCT multi stakeholder summit and relevant projects being undertaken with respect to access to data held by service providers, in addition to ongoing regulatory discussions about this issue.

The paper looks at a broad interpretation of what constitutes ‘data’ and identifies a number of policy questions and challenges that arise from the operational use of information by various actors. Additionally, recognizing the work being undertaken by the Transparency Working Group, we have sought to avoid focusing on questions relating to data about enforcement actions taken by services.

Types of data

From our initial work, the following types of relevant data were identified:

- Personally identifiable information (PII)
- TVEC
- Metadata relating to content
- Non-personal descriptive data (Hashtags, key phrases, titles of broadcasts, etc.)
- Contextual information about the sources of data

It is important to note that these categories are not mutually exclusive. PII for instance will cut across the other areas. TVEC may include the PII of victims of attacks, metadata can include precise location data and the name of the

media creator, hashtags and media titles can include the names of victims. It is also important to note that, as above, that various service providers and other stakeholders may have different definitions of TVEC.

Data processing and activity

As well as identifying relevant types of data, the group identified a number of different scenarios where data may be processed by a service, or activity may lead to new data being available:

- Activity that results in TVEC being removed from a service for violations of terms of service (either through human review or machine identification);
- The retention and storage of removed data by service providers;
- The transmission of data between services, both in raw form or using hashing techniques;
- The storage of data by third parties as an intermediary between service providers;
- The development of machine learning models using training data in the form of TVEC;
- The receipt of data from government agencies and law enforcement; and
- Access to data by non-governmental third parties, including academics, journalists, and NGOs.

Policy issues

As international legal frameworks and policy proposals relating to data held by services evolve and the technological landscape becomes more complex, a wide range of questions arise about the legal frameworks governing TVEC-related activity by technology companies. The issue of TVEC (and content accidentally identified as TVEC) that has been removed, intersects with several different legal areas, particularly the frameworks governing access to non-public data, as well as the framework around how different jurisdictions define and determine TVEC at a content and actor level.

As new laws have been passed around the world, particularly those broadly concerned with data, privacy, and the removal of TVEC, questions arising from how to handle a broader desire to access and use TVEC (whether by

industry, research, academic, or civil society actors) have become more pressing. Greater legal clarity, either through legislation or regulatory guidance, can have a significant impact in addressing these questions and allowing further action to disrupt TVEC.

For example, the working group noted discussion about the potential consequences of the U.K.'s Counter-Terrorism and Border Security Act,¹ which sought to criminalize repeated viewing of terrorist content online but only provided a statutory defense for the work of academics and journalists. As such, the status of those working on technical tools, commercial threat monitoring services, or non-academic research remains unclear, as does the interplay of this provision and the distribution of content among service providers (whether in raw or hashed form).

At the same time, the interplay among privacy legislation (including the General Data Protection Regulation) (GDPR) and the processing, sharing, and analysis of data concerning TVEC has been cited by several stakeholders as being an area where greater clarity could potentially enable more to be done to disrupt TVEC, enhance transparency and accountability efforts, and support work done by academics and civil society.

In the case of GDPR, there is a need for policymakers, regulators, industry, and civil society to better collaborate to increase understanding of the personal data implications of processing and sharing TVEC. The GDPR includes provisions for the processing of personal data for the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties. This includes safeguarding against (and the prevention of) threats to public security² in addition to general conditions of processing of personal data (in the form of the sharing of personal data by platforms with researchers).

One major issue discussed was the legal framework pertaining to content that has been removed by service providers and is no longer public. The U.S. Stored Communications Act was cited by industry and civil society stakeholders as a significant constraint on providing third parties access to TVEC that has been removed (irrespective of use).

The 2020 "Video Unavailable" report from Human Rights Watch and the presentation of its findings to the working group raised concerns that some of the content that is being taken down and no longer available to third parties

represents evidence of serious crimes (like war crimes) which is impeding human rights investigations. The “Berkeley Protocol”³ is also a noteworthy contribution to this debate, highlighting the increasing importance of data from social media services in bringing to account those responsible for war crimes and setting out potential frameworks for an evidence “locker” system.

A paper from the Yale Genocide Studies Program’s Mass Atrocities in the Digital Era (MADE) initiative⁴ has taken up this issue and sets out a potential model for policy reform. The authors propose both amending U.S. law to permit direct sharing by industry with international bodies, but also a liability waiver for civil society organizations who may handle certain types of content.

The issue of antitrust and competition was also raised by working group members and has been cited in broader public debate, recognizing that as policymakers raise concerns about anti-competitive behavior there are also calls for the industry to deepen its collaboration and partnership on the issue of TVEC content. Strengthening and clarifying frameworks for industry collaboration that provide protection and guidance on these issues will be invaluable.

One potential model cited was the work done in the U.S. by the National Centre for Missing and Exploited Children (NCMEC). The organization has a defined statutory role in disrupting the use of the internet for purposes connected to child sexual exploitation, including acting as an intermediary for the distribution of discovered material to relevant authorities. In conjunction with NCMEC, other NGOs, including Thorn and the U.K.’s Internet Watch Foundation, have also established technological services to disrupt this activity. However, this is in part dependent on strong international alignment on the specific type of content at issue, which may be challenging to replicate in the TVEC space.

The international nature of technology

One of the most significant challenges for addressing online extremism is that while the flow of data is global legal frameworks are not.

A TVEC incident can occur in one country, content can be distributed both within and outside of that country (on services based domestically and abroad), multiple law enforcement agencies may be involved, and staff

from several continents might be part of the response from technology companies. Civil society, service providers, and researchers based in numerous countries may monitor and capture such content, relaying it to other stakeholders and the industry.

While the group did not identify a major conflict of law that was an obstacle to the sharing of situational awareness of a crisis akin to the work undertaken by GIFCT members, the risk of longer-term regulation that would impede the flow of data or create new conflicts of law was noted as a concern. For example, this could include distributing links to services where manifestos or other content is hosted or sharing the name of an attacker identified by media.

Proposals relating to proactive notification to government agencies of removed TVEC have been discussed in several jurisdictions but they pose questions both with regard to conflict of law and due process. The need for legal frameworks to clearly delineate where data sharing is based on due process (either through an emergency process or the standard route) or a proactive obligation is critical. These issues are already a factor in the Budapest Convention and discussions around the E.U.'s E-Evidence proposals.

The U.S. legal framework around removed content was cited as one example where international actors felt the legal framework did not adequately address the issues arising, such as the applicability of the Stored Communications Act or concerns around surveillance privacy, while uncertainty over how the Mutual Legal Assistance Treaty (MLAT) framework would apply in this space was also noted.

Finally, the group observed that the question of jurisdictional nexus is not always a factor in governments seeking access to TVEC data, particularly now that multi-lateral processes have begun to establish crisis processes that share information across different entities and not just those directly involved.

Transparency

While the group did not want to duplicate the work of the Transparency Working Group, the question of how legal frameworks related to the issue of transparency was unavoidable in our discussions.

One issue frequently raised in public debate has been the emergence of “referral units,” notably the U.K.’s Counter Terrorism Internet Referral Unit and Europol’s E.U. Internet Referral Unit, which make requests to service providers for content removal. The wider question of the legal frameworks governing the referral units themselves, including what standards govern their work and what due process and human rights protections were followed when assessing content/accounts has been noted in the groups’ discussions and in other forums. While several service providers publish some aggregate data on these requests, it was highlighted by some members of the working group that the best source of such data is the referral units themselves. There needs to be more clarity about the legal framework(s) under which referral units operate and the formal framework for publishing data of their own work that goes beyond the current approach where data is often primarily disclosed as part of political discussions on an ad-hoc basis.

The question of transparency by service providers with regard to the content they remove has also been frequently raised. While some services do currently publish data on their removals, the different types of data shared as well as the granularity and frequency of those reports can differ. These are issues that are being investigated by numerous forums including the Organization for Economic Co-operation and Development (OECD).⁵

Both issues are important to inform the public and the policy debate about what is currently happening, and as a result the GIFCT Transparency Working Group is tackling a range of issues in this space.

Areas for further work and discussion

Many of the issues discussed by the group are complex, engaging different types of regulation across multiple jurisdictions in situations where legal action may not be immediately likely. The lack of legal clarity and potential risks highlighted in the working group’s discussions are an illustration for policymakers of potential areas of future investigation and legislation. There are areas where the group’s discussions crossed over into topics discussed in other work streams, including the Transparency Working Group and the Crisis Response Working Group’s discussions about how to handle data during a content incident.

Broadly, the areas that would merit further consideration and discussion

can be summarized as follows:

- Dedicated legal and policy frameworks that set out the processes, responsibilities and protections for those involved in the disruption of TVEC use of the internet could bring many benefits, address uncertainty and set clear boundaries while protecting human rights;
- Policymakers should explore clear statutory provisions and safe-harbor protections to facilitate access to TVEC considered for action (including removals), either directly from service providers or through an independent third party. This is potentially a major benefit to a range of stakeholders, including expanding independent research and international accountability for criminal acts;
- Privacy regulators, including international bodies of such regulators and multi-stakeholder forums where they participate, can proactively provide guidance on the personal data implications of the work being done to address TVEC use of the internet, including public guidance on the circumstances in which companies, NGOs, and others can process and share TVEC without the consent of the individuals depicted, named, or otherwise identified in such content, as well as the associated periods data can be retained;
- These issues may also be addressed through explicit regulation or guidance relating to data retention of TVEC, as well as associated metadata;
- The value of expanded legal protections for TVEC data sharing under competition law should be investigated by competition regulators to encourage greater collaboration among industry members while ensuring the full spectrum of services benefit;
- Where legislation or regulation seeks to criminalize the viewing, storing, or transmission of TVEC, policymakers should consider how to provide legal certainty and protection for the full range of actors who have legitimate needs to access, analyze, and share this content, including service providers, academics, human rights investigators, and civil society (including people working in community archiving). The potential implications for free expression and impact on unintended actors are both noted as important issues to consider in this context;
- The legal framework surrounding due process and transparency practices followed by referral units is unclear and should be expanded upon to provide clarity and clear scope, while questions around the transparency of these units' use of their powers are also important to address; and
- As regulation in the technology space expands, the issues around conflicts of law and international legal frameworks should be carefully addressed to avoid unintended consequences and further fragmentation of the free, open, secure, and Global Internet.

Endnotes

1 Counter-Terrorism and Border Security Act 2019, UK Public General Acts 2019 c. 3, Part 1, Chapter 1, Section 3, [link](#).

2 Article 2(2d).

3 “Berkeley Protocol on Digital Open Source Investigations,” Human Rights Center, UC Berkeley School of Law, 2020, [link](#)

4 Olivia Mooney, Kate Pundyk, Nathaniel Raymond and David Simon, “Social Media Evidence of Alleged Gross Human Rights Abuses: Improving Preservation and Access Through Policy Reform,” Mass Atrocities in the Digital Era Initiative (MADE) Working Paper No. 1, March 2021, [link](#)

5 “Current Approaches to Terrorist and Violent Extremist Content among the Global Top 50 Online Content-Sharing Services,” OECD Digital Economy Papers, no. 296 (August 2020), [link](#)

To learn more about the Global Internet
Forum to Counter Terrorism (GIFCT), please
visit our website or email outreach@gifct.org.

