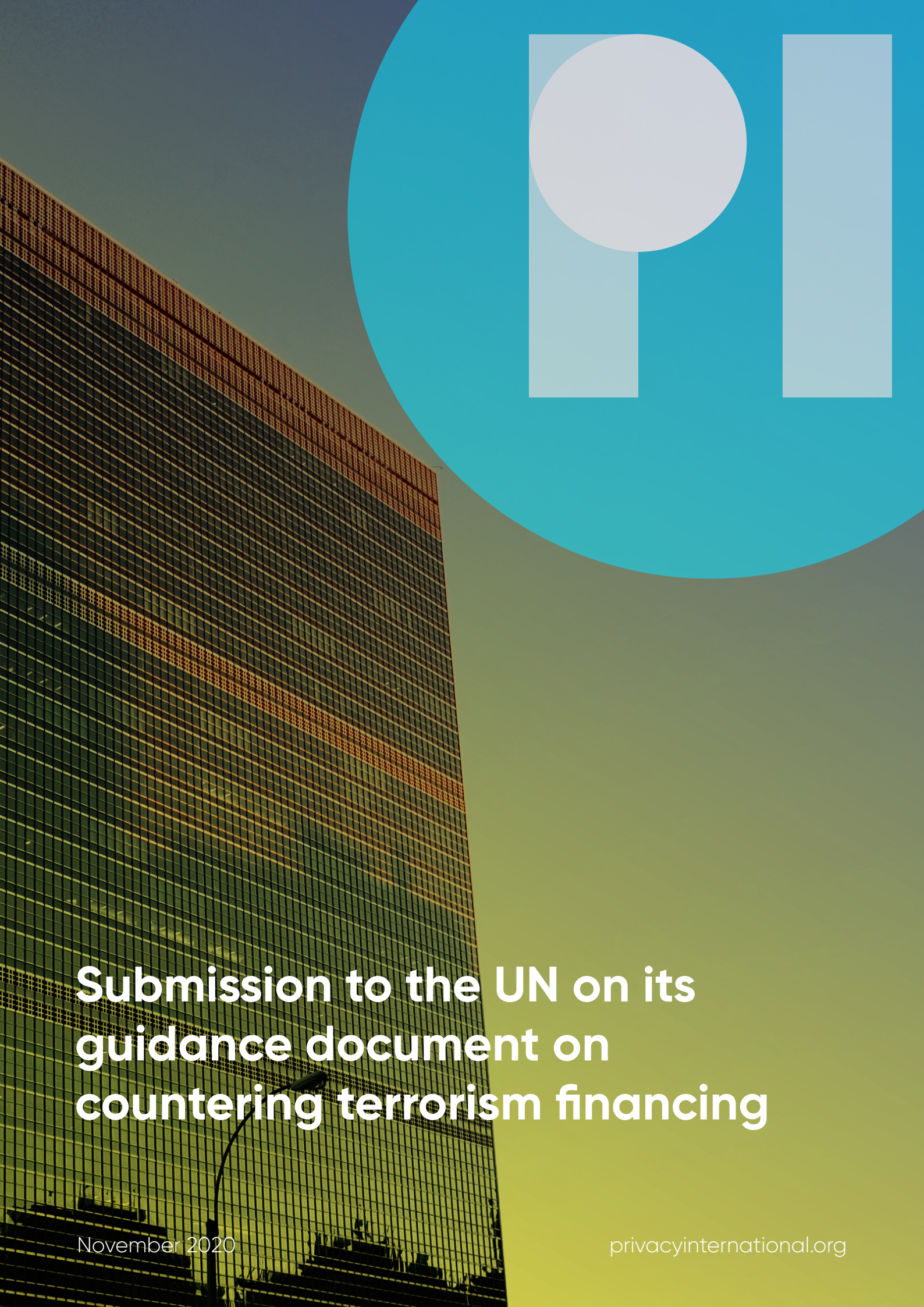


Submission to the UN on its guidance document on countering terrorism financing

November 2020

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters: our freedom to be human.

Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 2.0 UK: England & Wales. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;

You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright. For more information please go to www.creativecommons.org.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

Cover image: Daryan Shamkhali via Unsplash

PRIVACY INTERNATIONAL SUBMISSION TO THE UN ON ITS GUIDANCE DOCUMENT ON COUNTERING TERRORISM FINANCING WHILE RESPECTING HUMAN RIGHTS

1. Introduction

In this submission, Privacy International (PI) responds to the call for inputs to assist the UN Global Counter-Terrorism Coordination Compact Working Groups on "Criminal Justice, Legal Responses and Countering the Financing of Terrorism" and "Promoting and Protecting Human Rights and the Rule of Law while Countering Terrorism and Supporting Victims of Terrorism" in developing a guidance document intended to support Member States in their efforts to implement countering terrorism financing measures, in compliance with relevant Security Council resolutions, including resolution 2462 (2019), and in full respect of international human rights law.[1]

This submission focuses on: the extent of privacy interference in the processing of financial data; the role of the FATF's recommendations; support of government ID system; expansion of surveillance data; and intelligence sharing.

[1] See https://www.un.org/sc/ctc/news/2020/10/23/call-input-guidance-document-countering-terrorism-financing-respecting-human-rights/

2. Setting the context – financial data and its implications for the right to privacy

Financial data is some of the most sensitive data about people, revealing not only their financial standing but also factors like family interactions, behaviours and habits, and the state of their health, including mental health. While monitoring and regulating financial transactions are important for investigating and preventing terrorist acts and other serious crimes, it is essential that it is done in a way that does not endanger human rights.

Interference with human rights and capabilities of surveillance in this sector are many, but generally fall into the following stages:

- information requirements placed upon individuals and organisations, including identity documentation for opening and using accounts, requirements to explain the reasons of financial transactions (customer due diligence);
- generation of profiles and suspicious transaction reports on individuals' and organisations' activities based on the characteristics of the transactions;
- sharing of these reports and other financial data with Financial Intelligence Units, who then sometimes share data with law enforcement agencies;
- bulk sharing between and access to data by government authorities.[2]

These are often mandatory requirements that are not limited to investigation-led activities. In this sense, financial surveillance is markedly different to other forms of surveillance -where interferences to privacy must be on a case-by-case basis and authorised by an independent competent authority. Financial surveillance actively monitors transactions, generates intelligence on these transactions, shares data based on how the sector identifies 'suspicious activity' as opposed to being led by a law enforcement investigation.

[2] See https://privacyinternational.org/long-read/3257/how-financial-surveillance-name-counter-terrorism-fuels-social-exclusion

3. Role of the FATF's recommendations

The key regulatory framework that sets standards and monitors, but does not necessarily govern, the domain of financial surveillance is established by the Financial Action Task Force (the FATF.)[3] Though in theory it only sets recommendations, the FATF also has a monitoring function that evaluates countries' performance. While the FATF contends that implementation is left to national law and financial institutions, numerous governments and financial institutions claim that their actions to generate and collect information on people is necessary to be compliant with FATF's recommendations.

This was noted by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism in her 2019 report to the UN General Assembly. As the Special Rapporteur found:

> The FATF's mandate contains no references to international law, international human rights law or international humanitarian law. However, laws and policies related to the standards set up by the FATF address issues such as criminalizing and prosecuting terrorist financing, targeted financial sanctions, tackling the risk of abuse of the not-for-profit sector for terrorist financing purposes and, thus engage human rights at multiple levels. Their impact is all the more significant as States generally adopt domestic laws and policies that enable them to implement FATF standards, thereby leading to national 'hardening' of these otherwise soft law standards. In the Special Rapporteur's view, human rights implications linked to the development and implementation of these standards require sustained and in-depth attention.[4]

Despite some recent improvements, the FATF's recommendations has over the last twenty years contributed significantly to intense data collection, pre-emptive reporting and pre-suspicion profiling, that has driven the development

[3] The FATF was established in 1989 by the G7, to set standards and promote effective implementation of legal, regulatory, and operational measures for combating money laundering. In 2001 its remit was expanded to cover terrorist financing and other related threats to the integrity of the international financial system.
[4] See https://undocs.org/A/74/335

of privacy invasive banking practices and justified government identity systems globally.

4. Support of Government ID systems

The impact of rules surrounding terrorist financing extends far beyond the financial sector. In particular, meeting requirements on customer due diligence (CDD)[5] is a key driver of government identification systems worldwide, often used to justify disproportionate interference with privacy and other human rights, as well as resulting in social exclusion.[6]

While the FATF has started to acknowledge that ID requirements are imposing burdens and risk of exclusion, the FATF strongly insists on government-issued forms of identification, supporting the introduction of biometric identification systems and the retention of copies of identification documents. For example, while noting that challenges still remain, including related to the necessary technological infrastructure, the FATF supports the adoption of innovative, technology-based means to verify customer identities, including biometric registries.[7] Of particular concerns, the FATF highlights as positive cases India's

[5] Customer Due Diligence (CDD) is covered under the FATF's Recommendation No. 5. It requires that financial institutions identify the customer and verify that customer's identity using reliable, independent source documents, data or information. The institutions must identify the customer's identity using "reliable, independent source documents, data or information […] understand and obtain information on the purpose and intended nature of the business relationship, and conduct ongoing due diligence and scrutinise transactions."

[6] For an overview of the privacy and social implications of identity systems, see https://privacyinternational.org/topics/identity

[7] "One of the key challenges for these technology-led solutions is for countries and for financial institutions to build the necessary infrastructure – adequate readers and sufficient internet connectivity to allow for real-time or similarly reliable authentication of the captured biometric data with the central database, to ensure that the network of agents is technically equipped and capable to conduct identity verification, and to guarantee a satisfactory degree of certainty on whether the risk of identity fraud is adequately managed. The costs of using the real-time verification system can also be challenging for financial institutions. In addition, stringent data protection and privacy measures must be implemented across the system to ensure the data integrity, prevent data leakages that can facilitate identity fraud, including by money launderers and terrorist financiers, and to protect individuals' privacy and combat abuse." p14 2017 supplement

eKYC under Aadhaar[8], Colombia's national fingerprint database, and Pakistan's NADRA and SIM registration system.[9]

This reliance of government digital ID system needs to be carefully evaluated in light of the negative implications for human rights. The UN Secretary-General's roadmap on digital cooperation noted that:

> if digital identity is to become a trusted force for good and used for everyone, it has to be built upon a foundation of user agency and choice, informed consent, recognition of multiple forms of identity, space for anonymity and respect for privacy, ensuring that there is transparency when an individual's data are used by government and other entities.[10]

Further, the UN Secretary-General report on the role of new technologies for the realization of economic, social and cultural rights noted that:

> [d]igitized identity systems face great challenges regarding the security of the personal data collected, stored, shared and otherwise processed. Databases with information on millions of people are highly sensitive and attractive targets for attacks by criminal actors. Data breaches of any kind can facilitate identity theft, the consequences of which can be dire for the individuals concerned (A/HRC/39/29, para. 14). If the data collected contains biometric information, which is inseparably linked to a particular person and that person's life, the harms of data breaches can be irreparable.[11]

[8] Critiqued here: https://www.privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf
[9] Critiqued here: https://www.privacyinternational.org/feature/1100/identity-policies-clash-between-democracy-and-biometrics
[10] https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf
[11] https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_29.pdf

5. Expansion of surveillance data

The financial sector is facing changes, particularly as a result of counter-terrorism measures. PI notes the trend of financial institutions towards expanding the range of data they collect and analyse for Customer Due Diligence purposes, including to identify suspected terrorist financing. [12] The financial sector increasingly relies on "open source intelligence" (OSINT) and "social media intelligence" (SOCMINT). Other forms of identification by financial institutions that do not place a reliance of formal identification also results in a great deal of privacy violations, for example by looking at the entire contents of an individual's phone[13] or their social media accounts.[14] The abuses related the use of RegTech solutions have been documented such as those surrounding World-Check.[15]

These sources of personal information are approached by the financial sector (including credit references agencies, and as well as law enforcement officials and security agencies) as being unproblematic from a right to privacy perspective. They argue that this collection and analysis of data have little impact on people's privacy as and when it relies "only" on *publicly available* information. This inaccurate representation fails to account for the intrusive nature of collection, retention, use, and sharing of a person's personal data obtained from public places and through social media.[16] As noted by the UN High Commissioner for Human Rights:

> The protection of the right to privacy is not limited to private, secluded spaces, such as the home of a person, but extends to public spaces and information that is publicly available (see CCPR/C/COL/CO/7, para. 32).

[12] In 2016 the Executive Secretary of the FATF noted that changing technology was a risk and opportunity: "In a time when teenagers can create false IDs on their computers in their bedrooms in minutes, the value of customer identification using photo ID cards is becoming increasingly limited. At the same time these teenagers – and many of us – are posting everything about ourselves on the Internet and through a myriad of devices, and are leaving a unique digital footprint. So we now have the possibility to exploit FinTech and RegTech to update and substantially improve customer due diligence." See: http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-international-financial-congress-july-2016.html

[13] See: https://privacyinternational.org/report/998/fintech-privacy-and-identity-new-data-intensive-financial-sector

[14] See: https://privacyinternational.org/feature/2323/fintechs-dirty-little-secret-lenddo-facebook-and-challenge-identity

[15] See: https://privacyinternational.org/press-release/2078/press-release-privacy-international-asks-thomson-reuters-if-it-will-stop

[16] See: https://privacyinternational.org/explainer/55/social-media-intelligence

> For example, the right to privacy comes into play when a Government is monitoring a public space, such as a marketplace or a train station, thereby observing individuals. Similarly, when information that is publicly available about an individual on social media is collected and analysed, it also implicates the right to privacy. The public sharing of information does not render its substance unprotected.[17]

Similarly, the European Court of Human Rights has long held that "there is […] a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life",[18] particularly when this data is systematically or permanently recorded.

6. Intelligence sharing

Faced with the transnational dimension of terrorist-related activities, UN Security Council resolutions have emphasized the need for international cooperation in information-sharing.[19] Notably, resolution calls upon member states "to intensify and accelerate the timely exchange of relevant operational information and financial intelligence" and recommends a range of measures to achieve this.[20]

PI recognises the importance and benefit of intelligence sharing in the context of preventing and investigating terrorism or other genuine, serious threats to national security. The organisation is concerned, however, that unregulated, unfettered and unwarranted intelligence sharing poses substantive risks to human rights and to the democratic rule of law.

In the context of detecting suspected financial transactions, the FATF requires all countries to have legal or regulatory requirements that mandate the reporting of suspicious activities. The FATF Recommendation No 20 requires the

[17] Report of the UN High Commissioner for Human Rights, Rights to privacy in the digital age, UN doc. A/HRC/29/39, para. 6.
[18] *Peck v. the United Kingdom*, no. 44647/98, § 57, ECHR 2003-I; *Perry v. the United Kingdom*, no. 63737/00, § 36, ECHR 2003-IX (extracts); and *Köpke v. Germany* (dec), no. 420/07, 5 October 2010).
[19] See, in particular, UN Security Council resolutions S/RES/1373 (2001), 2322 (2016), 2396 (2017), 2462(2019) and 2482(2019).
[20] UN Security Council resolution 2462(2019), paragraph 19.

reporting of incidents to a country's Financial Intelligence Unit. This requires internal monitoring at financial institutions to identify any unusual behaviour.

In 2015, the FATF argued that sharing of data is a key way of combating terrorist risks, including by recommending

> empowering FIUs and other competent authorities to improve the exchange of financial and other relevant information domestically and internationally in a timely manner. The ability to detect, analyse and share information about financial flows is essential to financial investigations. For terrorist-related cases, governments should be able to obtain relevant information from all sources more rapidly. To achieve this, countries should strengthen inter-agency communication among financial intelligence units, law enforcement and intelligence services; encourage spontaneous exchanges of information among countries.[21]

However, despite the plethora of data required and of reporting, the system is far from effective. 90% of Suspicious Activity Reports (SARs) from the private sector are not relevant to law enforcement investigations.[22] It is estimated that less than 1% of all global illicit financial flows are intercepted.[23] This raises significant doubts as to whether the financial surveillance and reporting currently being supported by the FATF is necessary and proportionate to the achieve the legitimate aim of preventing terrorism financing.

[21] See https://www.fatf-gafi.org/documents/news/fatf-action-on-terrorist-finance.html
[22] See https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact
[23] Europol reports 'Does crime still pay? Criminal Asset Recovery in the EU - Survey of Statistical Information' https://www.europol.europa.eu/newsroom/news/does-crime-still-pay and 'Why is cash still king: a strategic report on the use of cash by criminal groups as a facilitator for money laundering' https://www.europol.europa.eu/content/why-cash-still-king-strategic-report-use-cash-criminalgroups-facilitator-money-laundering

7. Conclusions

Based on the above considerations, PI would like to recommend that in developing a guidance for UN member states, the UN Global Counter-Terrorism Coordination Compact Working Groups:

- Confirm the prominence of international human rights law, including the right to privacy, in relation to the collection, processing and sharing of financial information;
- Describe in details Member State's obligations under international human rights law, including when taking measures to implement the FATF's recommendations;
- Map and spell out the safeguards required to ensure protection of the privacy and the personal data of individuals concerned;
- Consider the privacy and security risks associated with some of the technologies deployed in this sector (particularly those processing biometric data);
- Consider the broader context into which surveillance of financial transactions takes place and the human rights consequences of imposing ID requirements;
- Identify the legal and other safeguards to regulate information sharing of data, particularly across jurisdictions.

Further, building on this initial public call for input, PI encourages the Working Groups to proactively seek to consult civil society and experts in the next stages of development of the scope and content of the guidance note.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).