PRIVACY INTERNATIONAL

# Submission for the report on 'soft law' by the UN Special Rapporteur on counter-terrorism and human rights

June 2019

PRIVACY INTERNATIONAL

30 June 2019

# Submission for the report on 'soft law' by the UN Special Rapporteur on counter-terrorism and human rights

Privacy International welcomes the consultation initiated by the UN Special Rapporteur on counter-terrorism and human rights on the impact on human rights of the proliferation of "soft law" instruments and related standard-setting initiatives and processes in the counter-terrorism context.

Privacy International is concerned that some of this "soft law" instruments have negative implications on the right to privacy leading to violations of other human rights. In this submission, the organisation focusses in particular on the measures adopted by the Financial Action Task Force (the FATF.)[1]

## 1. Setting the context: surveillance of financial data

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;

[1] Among the other bodies identified by the UN Special Rapporteur in her call for contribution, Privacy International is also concerned by the lack of transparency of the Shanghai Cooperation Organization. We understand that on 25 March 2019, CTED and the Regional Anti-Terrorist Structure of the Shanghai Cooperation Organization (RATS SCO) signed a Memorandum of Understanding "aimed at enhancing the strategic framework of cooperation between the two entities". The MoU, as described on the CTED's website, "provides, in particular, for enhanced information exchange on counter-terrorism". We plan to write to the CTED to seek more information on the content of such MoU and on the due diligence test to ensure sharing of intelligence does not result into violation of privacy or other human rights.

- sharing of these reports and other financial data with Financial Intelligence Units, who then sometimes share data with law enforcement agencies;
- bulk sharing and access to data by government authorities, such as when the U.S. intelligence services gained access to SWIFT[2], without any safeguards[3] or when generalised reporting is taking place to tax authorities.

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. Another difference is the key role played by the private sector (including financial institutions, but also involving state agents and other actors).

The practices outlined in this briefing are generally well established and have been in place for over twenty years. The sector is facing changes however, particularly in light of counter-terrorism. These changes are driven by:

- The changing nature of terrorist financing, with the amounts of cash required to conduct terrorist acts now very small;[4]
- Changing nature of data in the financial sector – data for the analysis, scoring and profiling of customers; and how this has led to a RegTech industry using data-driven techniques to meet with compliance;[5] and
- Changing use of technology to combat financial crime, including technologies like Artificial Intelligence.

Sectoral changes are also occurring with new entrants from the fintech sector as well as major platform companies entering with financial products (e.g. Apple, Google, Samsung, WhatsApp Pay), as well as innovations around blockchain (e.g. bitcoin, and the recently announced Facebook's Libra.)[6]

The key regulatory framework that sets and monitors, but does not necessarily govern, this domain is established by the Financial Action Task Force (the FATF.)

## 2. The role of the FATF

[2] See https://privacyinternational.org/feature/990/pulling-swift-one-bank-transfer-information-sent-us-authorities
[3] See https://privacyinternational.org/blog/1303/europes-privacy-commissioners-rule-against-swift and https://www.bbc.co.uk/news/technology-39606575
[4] See https://www.tandfonline.com/doi/full/10.1080/03071847.2019.1621479
[5] For more information on the fintech industry and its implications on privacy, see https://privacyinternational.org/topics/fintech
[6] See https://privacyinternational.org/long-read/3021/facebooks-new-cryptocurrency-libra-not-be-confused-libre

As the UN Special Rapporteur previously noted[7], 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.

Though in theory it only sets recommendations, it also has a monitoring function that evaluates countries' performance. Yet the FATF contends that implementation is left to national law and financial institutions. This often means that when concerns are raised, the FATF argues that the concern resides in national implementation and is thus not their domain; yet national implementation is monitored by the FATF.

The FATF's Recommendations[8] have been revised a number of times, often resulting in an expansion of the interferences identified above, including:

- in 2001 it added the targeting of non-profit organisations ('NPOs') as 'particularly vulnerable' to use by terrorists which led to concerns about 'de-risking' by financial institutions;
- in 2003 it added requirements around 'customer due diligence' (CDD) and Financial Intelligence Units (FIUs), which led to concerns around identity requirements, generation of vast data sets of financial transactions, and financial exclusion.

A positive change occurred in 2016, when following campaigns by civil society organisations and concerns expressed by the UN Special Rapporteur, the FATF revisited Recommendation No. 8 covering NPOs. It removed the claim that the NPO sector is “particularly vulnerable” to abuse. Changes were also made into how the FATF evaluates countries' implementation of Recommendation 8 - recognising the “chilling impact that regulations may have and not discouraging legitimate NPO activities”.

## 3. The FATF and Identity

The impact of rules surrounding money laundering and terrorist financing extends far beyond the financial sector. In particular, meeting the FATF requirements on customer due diligence is a key driver of government identification systems worldwide. Identity requirements lead to interference with privacy and other human rights, as well as social exclusion.[9] For example Privacy International’s research has revealed how in Chile, the lack of access to a national ID number leads to a high degree of exclusion, including but not limited to financial services[10]. Thus, the impact of the FATF recommendations far extends beyond the financial sphere.

### 3.1 Customer Due Diligence and its implications on privacy

[7] UN Doc. A/70/371.
[8] Full list of the FATF recommendations is here: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html
[9] For an overview of the privacy and social implications of identity systems, see https://privacyinternational.org/topics/identity
[10] See https://www.privacyinternational.org/feature/2544/exclusion-and-identity-life-without-id

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."

The problem that often arises is actually that governments go well beyond the FATF requirements. "Industry feedback highlights a number of practical difficulties regarding identification and verification requirements, most of which arise pursuant to national legislative or regulatory requirements, and not the FATF Recommendations. For instance, in a normal CDD scenario, the FATF Recommendations do not require information to be gathered on matters such as occupation, income or address, which some national AML/CFT regimes mandate, although it may be reasonable in many circumstances to seek some of this information so that effective monitoring for unusual transactions can occur."[11]

Over the years the FATF recognised the need to address financial exclusion. Excluding some actors from using the financial system they govern (e.g. by imposing too rigid frameworks and rules re: identification) risks resulting in those actors using alternative systems.

According to the FATF, they introduced a Risk Based Approach (RBA) to introduce flexibility into an otherwise rigid framework. In 2017, a new guidance articulated CDD requirements to ensure that "financial institutions can effectively identify, verify and monitor their customers and the financial transactions in which they engage, in relation to the money laundering and terrorism financing risks that they pose."[12]

The three core elements of "identification", "verification" and "monitoring" are intended to reinforce each other, so that the "financial institution builds knowledge of the customer".

Despite the language on RBA and financial inclusion, the FATF strongly insists on government-issued forms of identification, supports privacy invasive biometric identification systems and demands retention of identification documents raising risks of abuses and data breaches

- ***Reliance on government-issued identification documentation***

The FATF 2017 guidance recognises that "one of the main obstacles to providing appropriate regulated financial services or products to unbanked customers is their

[11] 2017 guidance, paragraph 67.
[12] See para 61 2017, Recommendation 10.

lack of reliable identity documentation and data verification. "[13] However, the FATF argues against an exemption approach.[14] As such, the revised Recommendation does not modify the basic CDD requirements. Rather they clarify only how the broad RBA principle relates to the implementation of CDD measures.[15]

- ***Reliance on biometric identification systems***

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.[16] Of particular concerns, the FATF highlights as positive cases India's eKYC under Aadhaar[17], Colombia's national fingerprint database, and Pakistan's NADRA and SIM registration system[18]. At least two of these systems have been critically analysed by civil society.

### 3.2 Suspicious transaction reporting

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 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

---

[13] See http://www.fatf-gafi.org/publications/fatfgeneral/documents/financial-inclusion-cdd-2017.html

[14] "In a financial inclusion context, newly banked and vulnerable groups often conduct a limited number of basic, low value transactions. Hence, they may present a lower ML/TF risk and this could appropriately be recognized as such by the risk assessment. However, it is important to keep in mind that underserved clients represent a very heterogeneous category with very different risk profiles in different jurisdictions. As a consequence, they cannot be classified as lower risk clients solely on the basis that they are low income individuals, who have recently been integrated into the formal financial system. Countries will need to clarify if and under what conditions and for which type of products and transactions low value clients can appropriately be subject to a simplified AML/CFT regime."

[15] Para 63 2017 guidance.

[16] "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

[17] Critiqued here: https://www.privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf

[18] Critiqued here: https://www.privacyinternational.org/feature/1100/identity-policies-clash-between-democracy-and-biometrics

communication among financial intelligence units, law enforcement and intelligence services; encourage spontaneous exchanges of information among countries."[19]

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.[20] It is estimated that less than 1% of all global illicit financial flows are intercepted.[21] 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.

### 3.3 Investigation and surveillance

The FATF Recommendation No 31 envisages wide surveillance powers to competent authorities investigating terrorist financing. Investigators must have access to "all necessary documents and information" related to these types of offenses, and are able to use investigative techniques like "undercover operations, intercepting communications, accessing computer systems and controlled delivery." Furthermore, investigators can "ask for all relevant information held by the FIU."

Some of these techniques, notably "accessing computer systems", are highly intrusive to privacy and may not be justifiable under international human rights law.[22]

There is no accompanying guidance to this recommendation. As a result, the FATF risks condoning surveillance measures which are not compliant with international human rights standards.

## 4. New technologies, new industry and new challenges

The FATF is not standing still. They are also actively watching innovations in fintech to ensure that it does not become the new cash.

In 2016 the Executive Secretary of the FATF argued that "the greatest risks of FinTech are often the lack of oversight or governance and the anonymity they can

---

[19] See https://www.fatf-gafi.org/documents/news/fatf-action-on-terrorist-finance.html

[20] See https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact

[21] 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

[22] Government hacking for surveillance has the potential to be far more privacy intrusive than any other surveillance technique, permitting the government to remotely and secretly access our personal devices and the data stored on them as well as to conduct novel forms of real-time surveillance, for example, by turning on microphones, cameras, or GPS-based locator technology. Hacking allows also governments to manipulate data on our devices, including corrupting, planting or deleting data, or recovering data that has been deleted, all while erasing any trace of the intrusion. For that reason the UN Special Rapporteur on freedom of expression observed that hacking constitutes a "new form[ ] of surveillance" as it permits states "to alter – inadvertently or purposefully – the information contained therein," which "threatens not only the right to privacy [but also] procedural fairness rights with respect to the use of such evidence in legal proceedings." (UN Doc. A/HRC/23/40, 17 April 2013, para. 62.)

provide, a characteristic they share with cash."[23] He also 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."

This indicates that they believe that additional personal data, beyond government-issued ID, can be used to develop and establish identity for the purpose of customer due diligence.

Privacy International notes that the trend of financial institutions is towards expanding the range of data they collect and analyse for CDD purposes, including to identify terrorist financing. The financial sector relies to a large extent 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[24] or their social media accounts.[25] These are approached by the financial sector (as well as law enforcement officials and security agencies) as being unproblematic sources of information for their intelligence activities. 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.[26] The European Court on 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",[27] particularly when this data is systematically or permanently recorded.

The use of vast new data sets, combined with technologies like Artificial Intelligence systems, creates new dangers. As Privacy International has seen with the field of predictive policing[28], the use of artificial intelligence and algorithms to make decisions on a limited data set can result in deeply prejudicial outcomes. Given the tiny amount of illicit financial flows that are detected, the danger is that using data and analytics in this context may reinforce existing bias in historical data whilst ignoring genuine criminality that doesn't 'fit the mould'.

---

[23] See: http://www.fatf-gafi.org/publications/fatfgeneral/documents/speech-international-financial-congress-july-2016.html
[24] See: https://privacyinternational.org/report/998/fintech-privacy-and-identity-new-data-intensive-financial-sector
[25] See: https://privacyinternational.org/feature/2323/fintechs-dirty-little-secret-lenddo-facebook-and-challenge-identity
[26] See: https://privacyinternational.org/explainer/55/social-media-intelligence
[27] *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).
[28] See https://privacyinternational.org/node/745

The abuses related the use of RegTech solutions have been documented such as those surrounding World-Check.[29]

These trends (and the related abuses) come together to form challenges that will make the guidance of organisations like the FATF more relevant and potentially more dangerous in the future. The way the FATF will seek to intervene and potentially regulated the fintech and RegTech sectors must be monitored.

## 5. Conclusions

The FATF is sensitive to criticism on privacy issues. The FATF President Roger Wilkins AO in October 2014 delivered a speech about de-risking, celebrating the use of biometrics in developing countries. And criticising the 'privacy lobby' for being rigid and ideological: "I think the rigid and dogmatic application of so-called 'privacy principles' have a lot to answer for."[30]

Concerns remain around customer due diligence, particularly around identity requirements and suspicious transaction reporting. The systems that the FATF celebrates involve significant interferences with rights, as exemplified in the India's Aadhaar. No identity scheme is truly universal, and it will always lead to some exclusions. Furthermore, given the scope of ID systems, they result in exclusion in areas beyond that of financial services (e.g. access to health and education).

Privacy International encourages the UN Special Rapporteur to make the following recommendations to the FATF:

- review its recommendations on CDD and ID requirements to ensure compliance with human rights, particularly in relation to the risks to privacy and to social exclusion;
- explore ways in which solutions not based on national ID schemes can be found for CDD purposes, particularly in emerging markets;
- review the recommendation on suspicion transaction reporting to ensure that it is compliant with human rights and that any sharing of personal information (within the financial institutions and with other authorities) is conducted in compliance with data protection standards;
- clarify that any investigative surveillance activities carried out by competent authorities comply with the principles of legality, necessity and proportionality and in particular to not condone forms of government hacking;
- ensure that the introduction of new technology in this space is compliant with the necessary and proportionate principles.

[29] See: https://privacyinternational.org/press-release/2078/press-release-privacy-international-asks-thomson-reuters-if-it-will-stop
[30] See: http://www.fatf-gafi.org/publications/fatfgeneral/documents/danger-illicit-markets-financial-exclusion.html

**PRIVACY INTERNATIONAL**

**Privacy International**
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

**UK Registered Charity No. 1147471**