FATF Secretariat
2, rue André Pascal
75016 Paris
France

Foundation
Human Rights in Finance.EU
PO Box 15673
1001 ND Amsterdam
legal@hrif.eu

May 3, 2024

Re: Comments of Human Rights in Finance.EU on the proposed revisions to R.16/INR.16

Dear readers,

Please find below the response of Human Rights in Finance.EU to the proposed revisions to R.16/INR.16.

Main suggestion: don't consult or tweak details but revoke R 16 completely

We will describe our arguments below. The recommendation is in its entirety not only completely outdated but its effect is a continuous unlawful infringement of human rights in violation of the Bill of Human Rights, the Resolution Privacy in a Digital Age and many similar constitutional ground rules in the local jurisdictions that 'voluntarily' choose to apply these "Recommendations'".

It is in practice of no use to comment on all the details and improvements and changes and the FATF play to 'invite' market players comment is a classic regulatory play trying to silence criticisms by saying: you had a chance to determine the outcome and by trying to create legitimacy through having a wide consultation cooperation. Legitimacy originates where we stick to the law. It doesn't come from forcing private players to transgress the law and human rights by default and invite them to comment on irrelevant details of the infringements they are supposed to execute.

Foundation Human Rights in Finance.EU

But first, let us tell more about ourselves. Human Rights in Finance . EU (HRIF.EU) is formally established in August 2023 as a civil society foundation. HRIF.EU protects human rights in Finance. For all kinds of economic transactions we focus on correcting and preventing human rights infringments that are the result of intrusive and improper regulatory rules or actions. In doing so, we focus on the complex domain of financial and anti-money laundering regulation and the behaviour of companies, regulators and supervisors where they go too far.

HRIF.EU is active since 2019

The actual inception of HRIF.EU dates back to the publication of a vital dissertation by Carolin Kaiser, titled: Privacy and Identity Issues in Financial Transactions: The proportionality of the European anti-money laundering legislation. This dissertation outlines and argues convincingly that in essence the European AML legislation is in violation of fundamental human rights and as such could be annulled by the European Court of Justice (considering all prior rulings and case law).

From that moment on, of the main founders of HRIF.EU Simon Lelieveldt (now the first Chairman) became active in promoting the respect for Human Rights in financial legislation and anti-money laundering legislation. He was the driving force behind the preparation of the joint letter of Privacy First and United Bitcoin Companies asking the Dutch Ministry of Finance to not approve rules which lead to rampant export of personal data. Yes, that was in 2019, and he wrote the FATF back then.

In order to maintain the effect of the recommendation but also maintain the privacy worldwide, he proposed applying the domestic format (using unique identifiers rather than personal data) to the new crypto INR 16 regime. The FATF responded by doing the reverse and claimed that crypto was so dangerous that even within the EU a international distribution regime for 'payment transparency' is needed. All other observations were laid aside.

The example is not unique. This is what the FATF does with consultations. FATF in essence incorporate comments to improve the mass surveillance character of its work. There's a range of scientific observations on that as well. FATF similarly tricked the Nordic states the same way (read: The FATF and Evolution of Counterterrorism Asset Freeze Laws in the Nordic Countries: We Fought the Soft Law and the Soft Law Won, by Aleksi Pursiainen). FATF then calls the human rights infringements: unintended consequences. And puts a symbol project in place to please the critics. But it has to stop and our aim as a foundation is to do so using all tools that we have in the toolbox to do so.

Ministries of Finance and respect for human rights are not a good combination

Technically, the FATF positions itself as a multi country governmental entity. And in some way you are, but what is interesting to note is that in order to fight crime, it is not the departments of Justice of countries, but the Ministries of Finance that are cooperating in the FATF-world. Those, in general do not really have a feeling for privacy or rule of law. They are intent on getting tax returns and law stuff is for lawyers at Ministries of Justice.

As a case in point. The Dutch Ministry of Finance tops the list of entities which are fined for GDPR transgressions.

Ministry of Finance / Tax Authority	12-4-2022	3.700.000
Ministry of Finance / Tax Authority	7-12-2021	2.750.000
BKR (credit register of banks)	6-7-2020	830.000
TikTok	22-7-2021	750.000
Unknown	30-4-2020	725.000
City Enschede	29-4-2021	600.000
VoetbalTV	16-7-2020	575.000
Ministery Foreign Affairs	6-4-2022	565.000
KNLTB (tennis union)	3-3-2020	525.000
Locatefamily.com	12-5-2021	525.000
DPG Media (Sanoma)	24-2-2022	525.000
Booking.com	31-3-2021	475.000

On 7 December 2021, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, DDPA) imposed a penalty of EUR 2.75 million on the Minister of Finance (Minister)
for the processing of personal data by the Tax Administration (Belastingdienst) in violation of the General Data Protection Regulation (GDPR) and the Dutch Personal Data Protection Act (Wbp).

On 7 April 2022, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, DDPA) imposed a penalty of EUR 3.7 million on the Minister of Finance (Minister). For the processing of personal data by the Tax Administration (Belastingdienst) in violation of the General Data Protection Regulation (GDPR) by maintaining a multitude of fraud-signalling records and databases, widely distributed and unchecked. There was a lack of legal basis, lack of limitation to purpose, inaccurate data, insufficient security measures and transgression of limitations to data storing, lack of involvement of Data Protection Officer.

Formal recommendations with informal coercion in the background, trying to be best in class

On paper FATF stuff looks real nice and formal. Well thought through. But the 'formal' structure of the FATF is accompanied by informal pushing and shoving of governments. In essence a peer pressure system is set up in which countries monitor each other and try not to reach the black or grey list. The monitoring system of FATF expands into operational oversight/supervision and all this without proper legal title.

In addition it is widely known that ambassadors of big countries do tend to also visit local countries' Ministries of Finance to explain the importance that is attached to those countries complying with the FATF-recommendations. Some economic benefits or disadvantages are explained and look what happens: the countries suddenly all want to be best in class.

In the Netherlands this Government policy paper in essence analyses the Dutch policy in view of the Evaluation of the Netherlands by FATF in 2021. The mechanism of a country trying to be the best in class is clearly at display here:

> "In 2021, FATF will assess whether the Netherlands complies with international standards for combating money laundering. For this, the Netherlands must demonstrate in detail that its regulations comply and that the measures it takes are effective. All parties with a role in preventing and combating money laundering in the Netherlands are thoroughly preparing for this evaluation together. We are preparing for the evaluation in close collaboration. In this role, we identify improvement points with stakeholders and strive to address them as much as possible before the evaluation. Ultimately, we aim to emerge from the evaluation as one of the leaders in combating money laundering."

Later on in January 2020 the Dutch Ministry of Finance literally said: we will go beyond what is required in order to get good grades from the FATF. Please note that we are speaking of collective/joint transaction monitoring initiatives as one of the ideas to innovate.

> We utilize innovative initiatives, such as a pilot Serious Crime Task Force, a joint working group of banks, supervision, and law enforcement on the theme of TBML (trade-based money laundering), and creating opportunities for joint transaction monitoring. With these initiatives, we go beyond what international standards prescribe. We refer to our ambition to be among the best in class in the evaluation by the FATF in 2021.

Well we did so and the European Banking Authority observed the mechanism in 2021 as well when looking at pre-emptive application of FATF suggestions in the Dutch and Swiss crypto-market:

> 164. The EBA has since observed that, in the absence of an EU-wide approach, there are indications that Member States, in anticipation of a forthcoming FATF Mutual Evaluation or to attract VASP business, have adopted their own VASP AML/CFT and wider regulatory regimes. As these regimes are not consistent, this creates confusion for consumers and market participants, undermines the level playing field and may lead to regulatory arbitrage. This exposes the EU's financial sector to ML/TF risk.

The result: we now do fully illegal transaction Monitoring in the Netherlands

What we really commend the FATF for is that you wrote this paragraph and box in your mutual evaluation report for the Netherlands of 2022. The reason being: we are currently doing an enforcement action against this pooled transaction monitoring mechanism and this is a good proof of the fact that the Transaction Monitoring Facility was alive and kicking. To please the FATF and get goody points. But did it have a legal basis?

121. In addition to public-public and public-private coordinating bodies, the Netherlands also has a number of private-private initiatives on AML/CFT. The below case study box outlines a recent initiative of the private sector to provide new insights into potential ML/TF across the Dutch banking sector.

Box 2.2. Transaction Monitoring Netherlands (TMNL)

Launched in 2020, TMNL is a joint initiative of five Dutch banks to collectively monitor their transactions to identify signals that could indicate ML/TF. Through collective transaction monitoring of combined transaction data, the primary goal of this initiative is to improve the detection of ML/TF by identifying unusual transaction patterns that individual banks cannot identify alone. As such, TMNL will focus on so-called multi-bank alerts. The privacy sensitive information of the transaction data to be exchanged between the banks and TMNL is pseudonymised. Currently, the utility is solely focusing on transaction information related to corporate clients.

Well, our government papers and policy discussions for 4 years since 2020 dealt with getting this TMNL-organisation a legal basis as it didn't have one and our AML-law would forbid this sharing of information. The Ministry of Finance knew this darn well as you can read from their papers:

> *Some banks are considering setting up joint monitoring through a specialized entity, also known as the TM-Utility or the initiative Transaction Monitoring Netherlands. The responsibility for this setup lies with the Wwft institutions themselves, but the Wwft obstructs a different organization of transaction monitoring in two aspects. This bill addresses these two points.*

So, in this evaluation. Did anyone of the FATF check this legal basis? Did our policy makers tell you that we are now in our 4th consecutive year of illegally harvesting, profiling, storing and pooling all B2C B2B and C2B transactions (4 billion per year)? Did any check the UN Resolution on Privacy in a Digital Age. The Bill of Human Rights. The European Charter of fundamental rights?

I guess not. You applaud the robust Dutch cooperation between private and public entities. You applaud the fact that Dutch governments do not intervene when companies go beyond the law in order to set up 'innovative' transaction monitoring utilities that by our own DPA are qualified as mass surveillance leading to such serious infringements of human rights that even if there were to be a law that stipulates the possibility of sharing info, such law would be unlawful under EU rules. Their letter dates from July 2023. But mind you: our council of State had also outlined the disproportionality of the measures/shared transaction monitoring.

We advise you to check up on the Netherlands and our law suit on this topic. And learn from it.

International resolutions do not become binding by themselves: Eu law still applies

Prior case law (C-402/05 P and C-415/05 P) clarifies that international agreements do not preclude the need to respect human rights: judiciary must review the lawfulness of Regulation 2023/1113. As it does not respect human rights it is unlawful and must be annulled.

The European Court of Justice has clarified in the Joined cases C-402/05 P and C-415/05 P that when Member States of Union bodies agree on resolutions on an international level, the European democratic safeguards remain in place:

> *Fundamental rights form an integral part of the general principles of law whose observance the Court ensures. For that purpose, the Court draws inspiration from the constitutional traditions common to the Member States and from the guidelines supplied by international instruments for the protection of human rights on which the Member States have collaborated or to which they are signatories. In that regard, the European Convention for the Protection of Human Rights and Fundamental Freedoms has special significance. Respect for human rights is therefore a condition of the lawfulness of Community acts, and measures incompatible with respect for human rights are not acceptable in the Community.*

Theerdict in the joined cases also outlines that the international rules cannot replace the constitutional principles of the EC Treaty:

> *The obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness which it is for the Court to review in the framework of the complete system of legal remedies established by the Treaty.*

When applied to the EU Regulation 2023/1113, to which Member States and European Union may have subscribed internationally in the context of the FATF, it follows from the above that the Judiciary must, in accordance with the powers conferred on it by the EC Treaty, ensure the review, in principle the full review, of the lawfulness of all Community acts in the light of the fundamental rights forming an integral part of the general principles of Community law, including review of Community measures which, like this regulation at hand, is designed to adopt 'Recommendations' of the FATF.

Many AML-people have the idea: is stuff is in law, AML-law is more important than privacy laws or human rights. But constitutional rights require balancing and if the balance isn't there, the infringement of human rights is not allowed. As a result, a Dutch risk management system SyRI was outlawed by a Dutch judge. The UN reported: Landmark ruling by Dutch court stops government attempts to spy on the poor. We advise the FATF to have a look into those mechanics.

Now, you may think: but Europe has implemented the wire transfer rule now so ware in the clear. Well, think again. The whole new AML framework was implemented without having done the prior human rights assessment under article 65g of the 4th AMLD and without having checked it it was proportional. The EU impact assessment said:

> No evaluation of the existing AML Directive has taken place to date prior to the preparation of the present impact assessment (see annex 4).

Human Rights Defenders Resolution

At this point in our feedback note, we point you to the recent Mini-course in human rights, which is made for all companies that think that stuff in EU law and FATF recommendations needs to be blindly followed. Bottom line: no one has to infringe humen rights and any fine can be taken to court using the UN Human Rights defender resolutions and relevant constitutional charters. And you can choose to stick the THE U.N. FRAMEWORK FOR BUSINESS AND HUMAN RIGHTS and explain you are not willing to infringe human rights.

Help, they are going to fine us, we must obey, resistance against FATF is futile!

Next up governments, bosses and managers may be going sour on you and say that the company risks being fined and there must be compliance. Well, that gets you to article ten. It's little known, and also quite new to me, but it is exactly the perspective that I applied in the Bitonic showcase.

If you wish to, if you sense that rules are disproportional and you can make a good case, this article 10 is going to be your way out against any opressive financial regulator or supervisor.

JUST SAY NO !

Use the fine to your advantage by considering it a punishment as identified in article 10 and refuse to pay. Take the oppressive supervisor to court.

Article 10

No one shall participate, by act or by failure to act where required, in violating human rights and fundamental freedoms and no one shall be subjected to punishment or adverse action of any kind for refusing to do so.

Well how do I say no in a smart way then?

The way to say no depends on the topic at hand. But rest assured, there is always a legal angle that represents the human rights and ethics that need to be protected. Start with the Human Rights Declarations. Follow on to other UN resolutions. Google "PROTECT, RESPECT AND REMEDY": THE U.N. FRAMEWORK FOR BUSINESS AND HUMAN RIGHTS

We are a legal person, the FATF is not ; Why does the OECD find hosting the secretariat to be apt?

A fun fact that we have outlined often. You as the FATF do not exist. You are a legal ghost. We as a foundation are a legal entity. That doesn't mean we can easily get bank accounts. The FATF work makes this impossible. But you as the FATF can by definition never be onboarded as you don't exist. You don't have a LEI. You are posturing as a nice international organization but act as a project group under the veil/shield of the OECD. Which, dear OECD, is something you must really review. Does it make sense, considering the OECD-guidelines on responsible business conduct, to provide secretariat services to a government project group that massively prescribes infringements on those rights as a policy business model?

What's wrong the INR16 then under EU law for example?

Ok. In essence the INR 16 is a prescribed mass data broadcasting idea. The personal data export obligation for these service providers form an arbitrary infringement of privacy, data protection of citizens and of the freedom to do business under the Charter of Fundamental Rights of the European Union. The reason being:

> Logic dictates that a generic massive and indiscriminate distribution obligation to send personal data for all customers and transactions to/via all business partners in the transaction chain is not necessary when the relevant information for citizens suspected of money laundering and terrorist finance is readily available at the request of law enforcement.

Now let's see where INR 16 came from. It was an idea to easily transfer personal data to other jurisdictions in order for local law enforcement not to be burdened with sending international requests for information and legal support. So pushing it out in the world was the easy way to do it. Well, that's 20 years ago. That's outdated.

The essence of INR 16 is a bulk surveillance and broadcasting regime. Which must be proportional under the law. Well, without individual legal title and actual police officers suspicion, there is litte legal title left to prescribe private actors the continuous sending of personal data as a nice to have thingy. We will explain the case law for you. We don't expect you to listen. But we do hope other readers may start to understand what Human Rights in Finance.EU is all about. In practice.

Data protection for bulk surveillance rules: case law

INR16 puts in place a one size fits all indiscriminate broadcasting regime for personal data and this can be functionally viewed as the sending part of a bulk surveillance and interception regime. As a result, the regular Court of Justice Case law comes into place with respect to such indiscriminate bulk interception and surveillance regimes.

In particular the Digital Rights Ireland case comes into play and the motivation behind the invalidation of the Data Retention Directive in Telecommunications domain:"

> ***Above all, the access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision sought to limit access to the data and their use to what was strictly necessary for the purpose of attaining the objective pursued.*** *The CJEU concluded that the directive entailed a wide-ranging and particularly serious interference with the rights in Articles 7 and 8 of the Charter, without having laid down clear and precise rules governing the extent of the interference and ensuring that it was actually limited to what was strictly necessary. Moreover, the directive did not provide for sufficient safeguards, by means of technical and organisational measures, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of those data.*

It can be concluded that important factors for properly devised surveillance regimes are:

- prior reviews of request carried out by an independent administrative body allowing limitation to what is strictly necessary,
- substantive and procedural conditions relating to access of competent national authorities to the data and their subsequent use,
- sufficient safeguards to ensure effective protection of the data against the risk of abuse and unlawful access.

All these safeguards are missing from INR 16. In essence it is an ongoing digital answer to a not-yet-asked and not-properly asked bulk interception request by all foreign intelligence services in the world (who can via local authority easily come into possession of the data as part of the end-to-end nature of the processing and their local competences to obtain the data).

In a similar vein the ECHR judgment in the Centrum för Rättvisa v. Sweden (application no. 35252/08) can in analogy be applied. The judgment in that case clarified that the existence of the surveillance regulation as such constituted an infringement of article 8 of the European Convention on Human Rights. The same holds true for Regulation 2023/1113. It's mere existence is already an infringement.

In the Swedish case a number of safeguards were in place, which mitigated the nature of the infringement. These end-to-end safeguards are missing as part of the legal context of INR16:

- there is no body as the Foreign Intelligence Court that authorises and evaluates a signals mission for bulk interception of data, with the aim to limit the scope of data interception to what is strictly necessary,
- there is thus no further limitation to carriers/means via which the data must be transmitted: instead the INR 16 allows a structure in which third party intermediaries also become the transporters of the personal data at hand (increasing the risk to the data subject),
- there is no supervisor such as the Foreign Intelligence Inspectorate assigned with the task to review and audit the signals intelligence chain,
- there is no limitation to the duration of the surveillance sending obligation, no ex post review of procedures and no supervisory mechanism for exported data.

In the Big Brother Watch Case the ECHR outlined the need for an end-to-end assessment of bulk surveillance regimes.

> *350. Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime (see also the report of the Venice Commission, at paragraph 197 above, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process).*

In our view, it is plain obvious, considering prior rulings of the Court of Justice such as Digital Rights Ireland in 2014 (C-293/12 and C-594/12), Tele2 Sverige and Watson and Others in 2016(C-203/15 and C-698/15) and Privacy International, La Quadrature du Net and Others in 2020 (C-623/17, C-511/18, C-512/18, C-520/18) that the FATF INR 16 does not pass the test of proportionality and lawfulness. Therefore it should be revoked.

<u>But we have the Wire Transfer Rule already in place in Europe so it's a done deal right?</u>
Again. Think twice. If a law or regulation violates the general principles of the Union's law in so far as it disrespects the fundamental rights it can be declared void. And with this recommendation it is clear there is a considerable tension with the norms in the UN Universal Declaration of Human Rights (article 12), The Human Rights Council Resolution 42/15 of 26 September 2019, and the Resolution 17/4 van 16 juni 2011, : Guiding Principles for Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (HR/PUB/11/04).

The 26 September 2019, Human Rights Council Resolution 42/15 on "The right to privacy in the digital age" stipulates:

> *2. Recalls that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality;*
>
> *6. Calls upon all States:*
>
> > *(d) To ensure that any measures taken to counter terrorism and violent extremism conducive to terrorism that interfere with the right to privacy are consistent with the principles of legality, necessity and proportionality, and comply with their obligations under international law;*
> > *(g) To consider adopting or reviewing legislation, regulations or policies to ensure that business enterprises fully incorporate the right to privacy and other relevant human rights into the design, development, deployment and evaluation of technologies, including artificial intelligence, and to provide individuals whose rights may have been violated or abused with access to an effective remedy, including reparation and guarantees of non-repetition*
> > *(j) To refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way, and to protect individuals from harm, including that caused by business enterprises through data collection, processing, storage and sharing and profiling, and the use of automated processes and machine learning;*
>
> *8. Encourages all business enterprises, in particular business enterprises that collect, store, use share and process data: (a) To meet their responsibility to respect human rights in accordance with the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, including the right to privacy in the digital age*

It is clear that many FATF recommendations and certainly this one on Payment Transparency, which prescribes unnecessary personal data export to all countries in the world to companies, is in sharp contrast with the above. In this respect it should be noted that a government supervisory task is also attributed to the industry players by peer pressuring their competitors into compliance. FATF thus encourages business companies to take steps that interfere with the right to privacy in an arbitrary way.

The FATF recommendation makes it impossible for companies to abide with their responsibilities under human rights and this Regulation at the same time. Resolution 17/4 of June 16, 2011: Guiding Principles for Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (HR/PUB/11/04) outlines:

> *11. Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.*
> *13. The responsibility to respect human rights requires that business enterprises: (a) Avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur; (b) Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.*
> *14. The responsibility of business enterprises to respect human rights applies to all enterprises regardless of their size, sector, operational context, ownership and structure.*

And there is more….
Well, let us stop here. There is so much more to explain, but we are running out of time. We compliment all the readers that made it to this part of our feedback.

We are pretty sure you at the FATF understand our point. Our vision for the future is:

- the FATF project can be disbanded and if it needs a new place to live it can be replaced by an international organization that starts with constitutional grounds/reasoning based on human rights values instead of the norms of Ministries of finance as tax collectors who use the presumption of guilt as their main perspective onto the world,
- the OECD should not host the FATF secretariat as the FATF infringes on human rights by default and this is not in line with the constitutional duties and role of the OECD
- the Dutch massive data pooling and transaction monitoring at TMNL demonstrates the cause and effect of FATF peer pressure and coercing; just to please the FATF Dutch banks are now violating human rights for 4 years in a row, legal proceedings will determine their liability and once this is done, we will most certainly hold the FATF liable as well,
- the R16/INR 16 can be revoked as outdated and leading to unlawful transgressions.

Good luck with the further infringements on human rights and the FATF work. We rest assured our response will be filed in the digital garbage can. But still these are points to make.

With kind regards

Simon Lelieveldt
Chairman
Human Rights in Finance . EU
(digitally sent).

Annex 1: Response in 2019 on consultation to add crypto to INR 16.

G20 and FATF should not infringe on the human right to privacy by prescribing mass surveillance for virtual assets !

Over the past weeks, I have been sounding the alarm as to the envisaged FATF-recommendations in the area of virtual assets. Essentially they require the private sector to build in a privacy leaking front-door in all blockchain applications, so that law enforcement officials in the whole world will have useful information already available nearby (rather than having to ask for it when need arises).

While at first I merely looked at it technically, seeing it as a disproportional silly measure by regulators who don't understand blockchain technology, over the past weeks I have learnt that it could also be viewed as part of a larger debate on the human right to privacy. People sent me more information on this matter including this dissertation (link: M. Wesseling: mustread!).

The dissertation outlines how a similar measure in the banking domain (the travel rule) was first rejected in US congress, to be adopted within weeks after the 9/11 attack. The dissertation also shows the mechanism of depolitization: making something a technical 'thingy' in order to avoid the true political debate on public interests that need to be balanced.

State vs citizens: police versus privacy

What is at stake here is a political debate on the degree of surveillance measures that a society needs to prevent criminality versus the degree of human privacy and freedom that people need to live a dignified live in which they can communicate freely and are innocent until proven guilty (and not the other around).

Let's have a close look at the two fundamental public policy issues at stake:

The human right to privacy in a digital age

Under UN Resolution RESOLUTION 28/16 (the right to privacy in the digital age), article 8.2 of the European Convention on Human Rights and the EU Court decision on data retention (ECLI:EU:C:2016:970) the EU understanding on mass surveillance of personal data of innocent persons is that it may very well constitute a violation of the right to privacy in cases where it is disproportional and no sufficient safeguards are in place.

However, the human right to privacy is often not taken into account when developing anti-terrorist policies. Scientific evaluations of the implementation of such policies outline that social side effects, such as excessive reporting of transactions and privacy of citizens, (often) remain underexposed in public discussions. Similarly a recent dissertation in the Netherlands clarifies that, when applying the EU Court of Justice criteria to the European Anti-Money Laundering Directive, 17 infringements of human rights can be identified.

Upcoming FATF-proposal to prevent fraud/crime/terrorism and apply broad rules to virtual assets

This is exactly what is at stake with a recommendation that is phrased in paragraph 7b of an interpretative note for Recommendation 15 of the FATF.It requires all private sector entities to register and submit the names of the parties participating in a virtual asset transfer to all counterparts in the value chain. This is not based on suspicion of criminal behaviour but required as a standard data export for all use cases and customers transferring virtual assets.

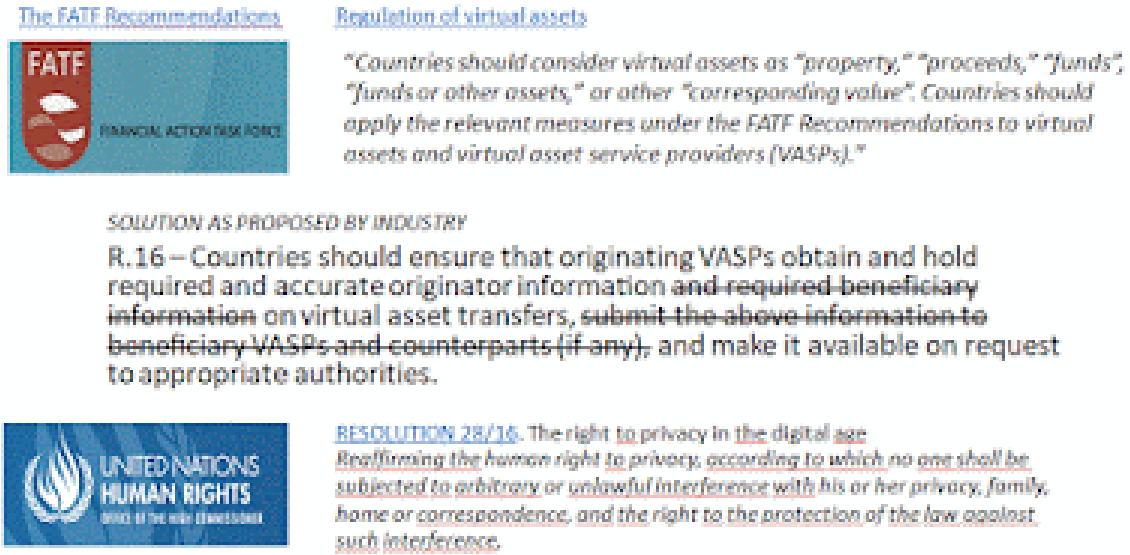
The virtual assets are defined as all non-regulated digital representations of value which may be transferred or held:

‘..countries should consider virtual assets as “property,” “proceeds,” “funds”, “funds or other assets,” or other “corresponding value”.

As such the rule effectively requires private sector market players to develop a messaging system (and adapt internal systems) to make sure future blockchain applications also functions as a structure of mass surveillance. However, any law enforcement official may obtain the relevant information on a case-by-case basis with a proper legal warrant at the individual organisation involved in a virtual asset transfer. The proposed rule constitutes an unnecessary measure that brings personal data of innocent people into the public domain, without any further proper guarantees for its treatment.

The rule has met with very heavy push back during a private sector consultation (in Spring 2019) due to its incompatibility with privacy laws and its unclear definition. The FATF members did not take this into account. Therefore, in the Netherlands, the NGO Privacy First joined the initiative of a group of virtual asset service providers (VBNL) to urgently request the Dutch Ministry of Finance to not approve the proposal. This has not lead to any further response.

What disturbs me in the process, is that the private sector has effectively formulated an adapted wording which would balance the two public policy interest more properly (see the redacted statement in the graphic below). But FATF-officials and governments appear to ignore it.



The public policy train moves on towards the G-20, without due process / democratic controls in place

Right now, the process underway is one in which we will see all kind of news reports about the G20 Ministers of Finance discussing and deciding on virtual assets. We will see the FATF adopting its rule in their 16-20 June meeting. And then the G-20 heads of state adopting it in Osaka. There will be many news bulletins and spins outlining how important and good these steps are. And the FATF will be complimented for their laudable work in this area. But don't be fooled by the spinning.

It is important to note that there has not been a sufficient and proper political debate on the balance between human rights and anti-terrorism measures. And as we already have Human Right Treaties in place outlining that mass surveillance and retaining of data of innocent people are a human right infringement, we can only conclude that our Ministries of Finance and Governments are about to make a historical and major mistake that violate their own commitments to privacy. There is no reason to boast about that.

Are all governments and private sector players benevolent forever?
What is lacking is the fundamental helicopter view on the relation between states and their people. For this I refer to yesterdays blog post, outlining the fundamental considerations that led Phil Zimmerman to develop encryption tool Pretty Good Privacy for the people:

> *"Zimmerman outlined one very significant theme during his speech. He noted that the assumption of a continuous benevolent government is not realistic. Governments come and go, some may be more democratic than others and even strong democracies may turn into dictatorships, depending on the circumstances. It is therefore important to design society, governments and the technologies that we use to manage society, guarantee that a balance exists between the powers of government and those of the public. The public, the people should always be allowed to remain digitally out of sight of government. Such a robust structure would be important to ensure a fair treatment of the people over a long period of time."*

It is too bad, that our governments appear to be unable to properly balance the political interests at hand. Reality is that we do not live in paradise: both governments and market players may have ill intentions and we should be open to that fact of life. In this respect it is clear that a range of private sector players provided more than one elegant suggestion to help with the criminal perspective, while still protecting it. Why would there be a reason to ignore this?

I do understand the dynamics however. In the words of Ian Grigg:
'It's hard to have a serious discussion on terrorism. It's too much of a magic password that shuts down critical thinking.'

What's up next is, that we will need to resort to national and supranational courts to re-address this issue and correct our governments. Because like it or not, the future of our democracies is at stake.

Annex 2: Professional background of reviewer and response to FINCEN Consultation early 2021

Introduction and response by Simon Lelieveldt, founder of Human Rights in Finance.EU

Now let me introduce myself further. I am writing in my professional/personal capacity and driven by a personal motivation that is reflected in the seal/logo and motto in the right upper corner: the NOW is the PAST is the PRESENT is the FUTURE. The moto is imprinted, using an old coin press, upon a wooden coin, made out of a 130 year old tree that stood on the Amsterdam exchange square. The tree, an Elm, witnessed time passing by and the development of society and financial markets. It symbolises the value I attach to cherishing history, learn lessons and use those learnings for todays developments. I hope you may appreciate my reflections from this perspective and rest assured, I'll get to the actualities of FATF and European privacy discussions in due time.

Professionally, I started out my career In as an industrial engineer in the financial sector by documenting and publishing a study on electronic payments (EFTPOS) regulation in 1989. In my research I revealed that the US Intelligence agencies had been pushing DES to become aninternational standard. At the time I did not have the ability however to put this finding into a broader perspective. However, more recently it became clear from the Crypto AG case that it was part of a long standing practice in which the US was actively pushing backdoors in technology, to ensure continued surveillance of all citizens and governments of the world. I think it is fair to say this is indeed the 'Intelligence coup of the century'.

Since then I embarked on a professional career starting out at ING/Postbank, moving on to become a policy analist at the central bank, charged with developing supervisory frameworks for electronicmoney in the 1990s. By the time that I contributed to European legislation and supervision for electronic money issuers, your organisation, FINCEN seemed to have made a strategic decision toposition itself as the go-to supervisor for all kind of modern payments and e-money. Although I think such a move may be analytically unsound and undesirable, I also view this as a natural reality ofinstitutional power politics. It is up to citizens, politicians, courts and private sector organisations to push back and hence my reflections in this letter.

Next up in my career, I worked extensively in the payments policy department of the Dutch bankers association. As such I was quite involved in the international rulemaking for banks and actually wrote the Dutch implementation guideline for the FATF7-rule (the origin of the travel rule). I was also a close witness to the SWIFT privacy incident and subsequent discussions on the EU privacy shield. Later on I moved towards a role as head of the department on financial markets and bank supervision of the Dutch Bankers Association.

What struck me in those days was the very anecdotal evidence and political framing arguments in discussions on money laundering and prevention of terrorist financing. It seems that 15 years later the situation hasn't changed and I would suggest the FINCEN to disclose and evaluate more precisely whether its role has been effective and whether this proposed rule actually adds any value when doing a broad analysis of costs/benefits. I'll get to that issue later.

Since 2011 I am active as an independent regulatory consultant and interim compliance manager for both government agencies and private sector entities. In this work, which mostly covers payment institutions, e-money and crypto, I try to reconcile justified regulatory requirements with business constraints/demands. And yes, the important wording is: **justified**.

Let me try and explain **why the FINCEN proposal is not justified: it continues the abuse of legal design flaws/choices that undermine human rights by misusing administrative law, financial supervision law instead of following penal law procedures which have proper safeguards for human rights.**

Sidestep: what use are consultations if you don't want to listen?

The Dutch scientist Dr. M. Wesseling has written an extensive and worthwhile dissertation on theinternational and European fight against terrorist financing and money laundering. The dissertation outlines that the US intelligence agencies have smartly used the momentum of the 9/11 attacks to get something they wanted: spying possibilities via the front door of financial transactions, bypassing formal legal and penal law safeguards, by pushing bank regulation and administrative rules. So what happened before 9/11?

A third important discourse concerned civil liberties. In 1999, the US Treasury proposed strengthened Know Your Customer (KYC) regulations. These proposals faced stiff opposition in the US Congress for anti-regulatory reasons, but the main issue at stake was concerns over privacy (Eckert, 2008, p. 213, Napoleoni, 2004, p. 219). The US Treasury received more than 200,000 negative responses to its proposal from all political backgrounds objecting to the proposed requirements for banks to obtain extensive private information (Donohue, 2006, p. 359). The KYC proposal was also criticized for being a potential source of mistrust and resentment of government, particularly among immigrants and minority groups, as well as an undesirable form of generalized spying and reporting on citizens (Cato Institute, 1999).

What FINCEN has seen in these 2 weeks of consultation will analytically not be very different from the responses that the US Treasury received more than 20 years ago. I would suggest that you include a review of those responses into your work, as they will undoubtedly be just as relevant.

Wesseling outlines how the 9/11 attacks changed the regulatory picture completely with civil liberties and human rights being:

The attacks of 11 September 2001 substantially changed the urgency and importance assigned to these different debates. The relative insignificance of the amounts of money involved in terrorism, the burden on the financial sector, the civil liberties implications of strengthened regulation, and the doubts about the use of UN economic sanctions, all became subordinate to the increased urgency of terrorism.

Although the 9/11 Commission would estimate in 2004 that the total costs of the attacks was between $400,000 and 500,000 and concluded that the costs of the attacks were relatively low compared to the amounts of daily financial transactions worldwide (2004, pp. 186-189), a radically different conclusion was drawn in the immediate aftermath of the 9/11 attacks.

Starving terrorists of their money had become a key objective within global governance. Likewise, financial regulation, such as Know Your Customer requirements, had been strengthened with little opposition from politicians, civil society or the financial and banking sector. Their current scope exceeds by far any previous initiative, making the contentious proposals of the 1990s look soft. Civil liberties, it was now widely accepted, had to be traded in if they constituted an opportunity for terrorists to 'hide'.

What I am saying here is that since 9/11 your organization is in a group think tunnel which has the effect of a religion or a cult. There is a dangerous liaison between intelligence agencies, tax authorities and financial supervisors which impose all kinds of intrusive rules under the FATF-umbrella as so-called: recommendations. Instead of revisiting the post 9/11 approach as a regulatory overshoot, the groupthink has remained intact as it comes in handy.

Or to put it differently. The US have since 2001 moved the angle of their intelligence attack from hardware based intelligence and surveillance to the informational front door that lies in financial transaction data. And this move is so useful and successful that US authorities are now even able to pull it off in broad daylight. Generations of bank personnel have become used to KYC/AML procedures that infringe on human rights. Now, from this perspective, it is clear that there is no way FINCEN will actually read or take on board any of the remarks in this consultation. As an institution the FINCEN has by now also brainwashed itself into believing its approach is valid and legitimate.

The big design flaw is that instead of penal law, the whole construct of administrative law and bank supervision law is misused to ensure unbridled and unchecked data flow of innocent citizens to authorities all around the world. So it is fair to say that the FINCEN has successfully contributed to maintaining a climate in which a legal design flaw is used in combination with a cultural ideology to hypnotise/brainwash financial professionals in acting in violation of clear human rights such as privacy and the right to be viewed as innocent until proven guilty.

Please see also Annex 1 to this letter (threadreader page - twitter feed) for a further explanation of the idiocy of still using administrative law when fine penal law structures exist and can be enforced to catch money launderers and terrorists on a spearfishing pull-request basis without the extensive data broadcasting and datamining requirements stemming from the pre-platform pre-big data age 2001. Then again, you could also read the 1999 consultation responses. All answers are in the public domain already. The real question is: FINCEN, are you listening. Really?

FINCEN violates human rights as a business model and should not force companies to join them

Under UN Resolution RESOLUTION 28/16 (the right to privacy in the digital age), article 8.2 of the European Convention on Human Rights and the EU Court decision on data retention (ECLI:EU:C:2016:970), the EU understanding on mass surveillance of personal data of innocent persons is that it may very well constitute a violation of the right to privacy in cases where it is disproportional and no sufficient safeguards are in place.

In this respect I can recommend the dissertation by Dr. Carolin Kaiser from 2018, outlining that – under todays case law and interpretations - the current EU regulation of KYC/AML may well be annulled by the EU Court of Justice. I am pretty confident that by analogy the same will hold true for US KYC/AML legislation when read against the UN Charter of Human Rights. But let us focus on the EU situation more closely.

Last month the European Data Protection Board issued an important statement outlining the importance they attach to protecting the human right toprivacy in particular given the intrusive money laundering procedures that have arisen all over the world.

The EDPB considers it as a matter of the utmost importance that the anti-money laundering measures are compatible with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, the principles of necessity of such measures in a democratic society and their proportionality, and the case law of the Court of Justice of the European Union.

The EDPB therefore calls on the European Commission to be associated to the drafting process of any new anti-money laundering legislation in its early stages, with a view to provide legal advice on some key points from a data protection perspective, without prejudice to the consultation by the European Commission in line with Article 42 of Regulation 2018/1725 at a later stage.

The EDPB is also ready to contribute to discussions within the Council of the EU and the European Parliament during the legislative process. Going forward, the EDPB stands ready to be involved and consulted in a timely manner by any European or international regulatory bodies or standard-setters, such as the Financial Action Task Force, currently chaired by an EU Member state, before issuance of the revision of their recommendations.

Coming back to the details of your proposed regulation. Human right treaties require that intrusive surveillance requires serious crime under human rights charters. **It can hardly be argued that just the sheer use of unhosted wallets for higher amounts is a demonstration of this serious crime. The suspicion should come from formal police officers doing their job, not from private sector players which are obliged to snitch upon their customers and broadcast their data into all kinds of databases without reasonable suspicion being present.**

Next up, you are also overlooking the fact that businesses are by themselves obliged to honour the human rights under the "Guiding Principles on Business and Human Rights: Implementing theUnited Nations 'Protect, Respect and Remedy' Framework", which were developed by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises. The Human Rights Council endorsed the Guiding Principles in its resolution 17/4 of 16 June 2011.

It should not be up to companies to reconcile conflicting legislative objectives. It is up to regulators to steer clear from conflicts of law and not impose undue human rights violations onto companies.

FATF: continuation of the ill-footed surveillance model

FINCEN is engaged in a regulatory experiment that has been agreed upon by the FATF in the summer of 2019 or 2020. Confronted with the new blockchain / virtual asset technology, the choice has been made to push the travel rule into the blockchain world. The US has used its leadership position of the FATF to push this agenda item through. Which essentially sums up 20 years of anti-money laundering policies worldwide.

In Annex 2 I have listed the blogpost with which I tried to warn the FATF/public in spring 2019 on the fact that pushing through a travel rule for crypto is just as useless as it was for banks back in the days. There is no sufficient quantitative evidence that any of those rules has really benefited finding criminals and preventing terrorist attacks (see the dissertation of M. Wesseling). It is a cost burden to all professionals in the financial sector and the resources spent could be better allocated directly to police forces or Ministries of Justice instead, as this warrants better protection of suspect individuals.

The recent evaluation of the FATF virtual asset travel rule clearly outlines the 2-step approach that is being taken. First force the travel rule upon registered/licensed players, then as phase 2 force them to verify the beneficiary of wallet transactions. This is a requirement which even goes beyond the R15 and R16 regulations for banks !!

If I read the FATF document correctly the FATF-members have agreed to not follow a similar policy line but to use the year 2020/2021 as an experimentation year. The 12-month review of the revised fatf standards on virtual assets and virtual asset service providers is clear that there is no real risk present:

> *53. However, jurisdictions did not consider that there was sufficient evidence to warrant changing the revised FATF Standards at this point at time. There was insufficient evidence demonstrating that the number and value of anonymous peerto-peer transactions has changed enough since June 2019 to present a materially different ML/TF risk. Further research could be undertaken with the VASP sector, academics and software experts and engineers to better understand the scope of the unregulated peer-to-peer sector.*

Yet, the document also gives a path to further experimentation per jurisdiction. If government authorities put the risk levels on high, they may start to experiment with additional regulations:

54. The launch of new virtual assets however could materially change the ML/TF risks, particularly if there is mass-adoption of a virtual asset that enables anonymous peer-to-peer transactions. There are a range of tools that are available at a national level to mitigate, to some extent, the risks posed by anonymous peer-to-peer transactions if national authorities consider the ML/TF risk to be unacceptably high. This includes banning or denying licensing of platforms if they allow unhosted wallet transfers, introducing transactional or volume limits on peer-to-peer transactions or mandating that transactions occur with the use of a VASP or financial institutions. As of yet, no common practises or consistent international approach have emerged regarding the use of these different tools. Accordingly, there should be further work undertaken on the extent to which anonymous peer-to-peer transactions via unhosted wallets is occurring, the approach jurisdictions can take to mitigate the ML/TF risks, the extent to which the revised Standards enable jurisdictions to mitigate these risks and to continue to improve international co-operation and coordination.

Right now we have seen the FINMA issuing regulations beyond the informational travel rule, coming down to verifying the beneficiary of transactions. And the Dutch Central bank has also made thisrequirement a (disputed) prerequisite in their registration process for crypto companies. I view the FINCEN rules as a part of the same process.

What FINCEN is thus doing as a regulator/contributor to FATF discussion is something which could be called agile regulation. Where usually companies may seek to roll out products in not yet definitive form, I would qualify the current world wide regulatory approach on crypto assets and the travel rule as an agile form of experimentation, at the cost of the private sector.

Government agencies do not only have a duty to not write or impose conflicting requirements upon their constituents but also to ensure their actions are coordinated. But as the FATF intermediary paper says: *As of yet, no common practises or consistent international approach have emerged regarding the use of these different tools.*

What you are proposing as FINCEN (and will be rolling out, as I fail to see any true intention of finding an optimal regulatory solutions) is an uncoordinated regulatory measure which will lead to increased cost in a number of different jurisdictions for an industry that is worldwide by nature.

The side effects of the approach is that FINCEN and other regulators are making sure that only larger well capitalised companies in the crypto space can survive (as they are faced with different costs in different jurisdictions). Both by nature and their effect, the proposed rule impedes innovation and leads to undesirable market structures.

FINCEN operational risk and failures

Now let's turn to the track record of FINCEN itself. I will be blunt in a Dutch way here. You fail to keep your records safe. For this rule it means that basically we can envisage that at some point in time hackers will have the possession of names/address of owners of bitcoin addresses. This is an impact beyond the Ledger hack (which was already scary). It is the equivalent of throwing all peoples bank account statements in the streets. Which cannot be undone and I don't see any appreciation of the operational/privacy risks that you create in this way.

The FINCEN-files leak shows that you will be unable to prevent this data from being safe. It also shows that FINCEN is unable to do its job properly. You are going after the crumbs on the table and leave the big money laundering industries and players untouched. Case in point: at present the US still has a President that may better be labelled the money launderer in chief. No FINCEN authority, no AML/KYC rules have been able to prevent this from happening.

US from inspiration to dystopian example?

Each moment in life encompasses all its previous moments as well as its future moments. That is the meaning of NOW is the PAST is the PRESENT is the FUTURE.

The FINCEN proposal is clearly born out of a tradition of illegitimate government action, spurred by overactive intelligence desires of the US. It is the second biggest intelligence coup in progress which may deter a whole innovative open source blockchain technology from maturing into beneficial society solutions. Because with these rules you are making virtual assets, distributed ledgers and digital tokens into data drones, to be automatically sent to government.

I find it quite ironic that the US, that saved the Dutch population from a dictatorial regime, that taught us about the importance of human rights, true democracies, freedom of speech, privacy and the importance of the presumption of innocence, is now the country that violates the values it has inspired into others.