PRIVACY INTERNATIONAL

# Submission to the Financial Action Task Force public consultation on FATF draft guidance on digital identity

November 2019

# INTRODUCTION

Privacy International welcomes this opportunity to submit comments to the FATF consultation. The draft recommendation is an improvement on existing guidance that we have reviewed.

We also welcome the calls of the FATF for accommodations that will relieve burdens upon individuals who are being excluded from the financial sector, as a result of the FATF's prior recommendations.

PI believes that identity systems must empower people. The initial question surrounding the development of any identity system has to be one of its purpose and need, and it's essential that the design of the system meets that need. At the same time, given the potential of an identity system to interfere with the fundamental right to privacy, the purpose should be clearly defined, legitimate, and such systems should be deployed only if there is not another less intrusive way to achieve the same goals.

Instead too often identity systems create risks for those who have access to an ID, as well as those who don't. These systems can exclude: for all the claims of universality, there will be some people who do not have access to an ID, or those who cannot use their ID, and are denied access to goods and services. ID systems can exploit: they link together diverse sets of information about an individual, and allow tracking and profiling. ID systems can surveil: giving the state and private sector a 360-degree view of the person. All three of these are made worse by function creep - the spread of an identity system to more and more aspects of people's lives.

Particularly as an ID system's role is to enable people to authenticate their identity to access financial services, it is imperative that an ID system is as inclusive as possible, and mitigate exclusionary consequences, which might be caused by economic, cultural, geographical, physical ability, or other factors.

As highlighted in Privacy International's research on identity and exclusion, mandating the need for identification - or one particular form of ID - to access

services leads to social exclusion.[1] Similarly, it has to be recognised that those who have difficulty getting the proof of identity are also those open to exploitation, as shown by Privacy International's research into the fintech sector,[2] and on the impact of financial regulations for example in the delivery of humanitarian assistance,[3] emphasising the importance of protections to be placed in a system.

To broaden inclusion in the system, we need to make sure that a broad range of diverse ways for people to assert their identity are permitted, as well as measures to improve accessibility (like, for example, real-world help and support contact points). To lessen the risks of exclusion as a result of identity systems, the situations that need a form of identification must be minimised – in particular, the introduction of a digital ID system must be stopped from leading to new uses of ID where currently there is no such requirement. If it is the case that identity is required, there needs to be a breadth of options available, not limited to one particular system. And not being able to provide an ID should never result to the denial of services such as health care, social protection and other essential benefits and services.

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 preventing crime, it is essential that it is done in a way that does not endanger human rights.[4]

---

[1] See https://privacyinternational.org/long-read/2544/exclusion-and-identity-life-without-id

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

[3] https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era

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

This is why PI believes that one of the most important solutions is to find ways of removing ID requirements. The FATF has started to acknowledge that ID requirements are imposing burdens – and while digital ID could help alleviate some of the exclusion that is occurring, fundamentally the exclusion is solved by removing the burdensome requirements where they are not necessary. The draft guidance does not go far enough on clarifying previous recommendations by the FATF; and while it takes a relatively progressive view of digital ID, embedded throughout the recommendations are hints that more expansive uses are recommended, that could shape the structure of identity for years to come.

## KEY AREAS OF CONCERN

The FATF must consider its outsized role that may come to determine the shape of how much of the technical and social infrastructure gets reshaped in the coming years.

The FATF play a huge role in the establishment not only of guidance but also in practice. This has immense ramifications for rights, including with regards to exclusion, unfair targeting, and privacy.

This was recently noted by the UN Special Rapporteur on counter-terrorism and human rights in her report to the 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."[5]

We welcome the call of the FATF for flexibility in national jurisdictions. Paragraphs 163-165 are helpful but considering FATF's other documentation and the regular conduct of national governments and financial institutions, that the FATF monitor, more is needed.

We also welcome FATF's consideration to financial exclusion and the disparate distribution of technology across societies, e.g. smartphones, and even how different technologies interact differently with different people, e.g. biometrics. (p138) However, it does not go far enough considering the enormous extent to which people still do not have access to the internet and to devices, let alone secure devices. This digital divide means that those most in need of financial assistance are not going to be able to access savings and some of the other advantages promised by digital accounts and fintech.

The only way this can all be resolved is if the FATF starts demanding that countries develop and adopt necessary safeguards and rules to protect people and their data from abuse. This is rich and dynamic discussion about the future of innovation and the protection of rights – and having the FATF in this discussion, including to provide clarity, would be welcome. Below we explain how this is increasingly urgent and use the FATF recommendation on digital ID as another instance.

The current soft language on 'it will be the responsibility of the Government to establish overall data protection and privacy framework in each jurisdiction' (p136) and that there are 'countries with limited data protection laws in place, without adequate mitigation measures in place, there could be greater risk of identity theft and cybersecurity risks, and trust in the system may consequently be lower.' As we explore below, i) it's no longer tenable for a standard-setting

[5] https://www.ohchr.org/EN/Issues/Terrorism/Pages/Annual.aspx and https://undocs.org/A/74/335

and monitoring organisation like the FATF to not 'recommend' *and* 'monitor' data protection and privacy safeguards, and ii) this is particularly urgent considering the technical designs and innovations the draft guidance explores, building on previous documents from the FATF.

Put more succinctly, the FATF's conduct has over the last twenty years given rise to a world of intense data collection, pre-emptive reporting and pre-suspicion profiling, that's driven the development of invasive banking practices and justified government identity systems globally. In recent years the FATF appears to have wisened to its influence and has called for flexibility even while it monitors. Now the FATF is firmly entering the domain of technology and innovation with this draft recommendation, it can no longer ignore the huge disparate effect it is having on the world, which is why we welcome the focus on inclusion and exclusion. We expect the same with fundamental human rights, including the right to privacy.

We are optimistic a positive role for the FATF can be found. With its focus on financial inclusion that takes into account levels of assurance (p110), this may broaden peoples' ability to prove the authenticity of their claims. If the standards are done right, and implemented properly, there are some advantages and improvements on the current situations.

## Infrastructure setting role of the FATF

The FATF guidance is, perhaps unintentionally so, a primary driver for identity systems. Numerous governments and financial institutions claim that their actions to generate and collect identity information on people is necessary to be compliant with FATF's global standards.

This is not a responsibility that the FATF has clearly owned. Even in the draft guidance the FATF claims "the FATF does not require jurisdictions to adopt any specific type of identity framework" (p132). Yet it is well aware. The FATF 2017 guidance recognises that "one of the main obstacles to providing appropriate regulated financial services or products to unbanked customers is their lack of reliable identity documentation and data verification." While exemptions would

be at a minimum a recommended course of action, the FATF documents argue against an exemption approach. As such, the revised Recommendation does not modify the basic CDD requirements. Rather they clarify only how the broad risk-based approach relates to the implementation of CDD measures.

Universal identification programmes therefore follow from FATF guidance. And at times the FATF is attendant to this, quite passively, in the content of digital ID while ignoring it plays in justifying large centralised national IDs (see p133).

We therefore welcome additional consideration placed into the thresholds, flexibility (p166) and application of ID based on risk, but the reality is that the structure of the FATF's standard-setting role is also a primary driver for disproportionate generation and collection of data through identity systems. This is evidenced in this draft guidance with immediate reference (in p167) to the 2017 guidance.

A final point on this: after much careful description of the identification and authentication process (p180), the draft document surprisingly states that authentication is the verification of 'who you say you are'. In reality it is not about the full chain including identity – it can be the verification of any claim, which may include 'who you say you are'. Identity itself may not be required in transactions, and even then, it may not be the identity of the account-named individual who is involved in the transaction itself.

## Standard-setting role of the FATF is challenging to privacy

The FATF set recommendations, but the monitoring function of the FATF is influential, even though it 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 its domain; yet national implementation is monitored by the FATF.

There is FATF documentation often speaks of flexibility:

"If a customer lacks a government-issued form of identification, for example, a financial institution may need to use other, more costly methods to verify identification, which could be a disincentive to serve certain customers. For some categories of potential clients, and especially for vulnerable and low-income groups, this creates an additional barrier to financial inclusion."

On numerous occasions the FATF has noted that flexibility in national application was not used by governments. This was originally noted in its review conducted in between 2005-2011, and again in 2017 the FATF reconfirmed that it was not being used by countries.

Even still, with an exemption its documentation continues:

"When a country decides to exempt certain natural or legal persons from AML/CFT requirements because they engage in financial activity on an occasional or very limited basis, the onus is on the country to establish that the conditions set out in the FATF Recommendations are met."[6]

But countries who wish to deploy national ID systems and use banking as the justification for doing so will not find it in their interests to apply this 'flexibility'.

The FATF does not provide sufficient incentives. Its 2017 guidance on customer due diligence and the risk-based approach in the financial inclusion context with the goal of encouraging countries to use the flexibility within the FATF Recommendations. It noted that:

"One of the main obstacles to providing appropriate regulated financial services or products to unbanked customers is their lack of reliable identity documentation and data verification. Low income individuals or displaced persons such as refugees, often do not possess the proper identification documentation and are therefore not able to meet "traditional" customer due diligence requirements. The risk-based approach allows for a certain amount of

[6] (p.51 2017 Guidance)

flexibility to provide access to basic, regulated financial products to a larger proportion of the population."[7]

The document noted hopefully that:

"FATF believes that the present Guidance will contribute to removing existing and perceived obstacles and clarify how to implement AML/CFT requirements, including the documentation requirements, in a financial inclusion context."[8]

The FATF contends the lack of government identification documents may lead to financial institutions requiring customers to use other, more costly methods to verify identification, "which could be a disincentive to serve certain customers."

Nonetheless, the FATF again argues against an exemption approach:

"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."

We are curious if in the two years subsequent to that 2017 document if the FATF, in its monitoring role, has seen indications of the adoption of positive flexibilities,

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

[8] p.40 2017 recommendations

or if countries have instead chosen to not introduce flexibility because of its requirement to 'clarify'.

## On digital ID

Digital ID systems, when innovative and purposefully designed, can lead to dramatic improvements on current practices, empower individuals, and lead to the reduction of risk and fraud. When properly designed, it can lead to the reduction of single identifiers, which have proven to be security and privacy points of failure.

A well-designed federated identity ecosystem has the potential to avoid many of these issues, for example by not having a centralised database or ID card and enabling the opportunity for creating multiple accounts with various Identity Providers. However, it remains the case that even such a system can be open to human rights abuses or open to exploitation of people's data. The design of such a system must be such that the risks are minimalised.

The identity ecosystem that is developed, and the economics of the system, must reflect this: for example, the source of income for identity providers must be from providing identity assurance services, rather than any other use of the data (with the appropriate Chinese walls and other measures in place within companies, if necessary).

There are technical solutions that can aid in the design of the system. For example, a federated system can make use of Zero Knowledge Proofs, which can be used to prove that a party has evidence or proof of an attribute without revealing that evidence or the underlying data. One of the great opportunities will be for the development of new innovations in these types of technologies, deployed in a real-world environment.

Technology, however, is never a panacea. It is also essential that all parties in the identity ecosystem, including relying parties are subject to appropriate regulation, certification, and standards.

## The challenge of addressing new technology

Acknowledging that countries are 'adopting innovative, technology-based means to verify customer identities, including biometric registries, FATF note that challenges still remain. We welcome that the FATF notes, in its 2017 supplement, that data protection and privacy measures must be implemented across the system:

"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."[9]

We also welcome that with regard to collection and storage of identity documents for five years (which we do not agree is necessary), the FATF notes that copying identity documents could be avoided in some settings because some countries have fraud concerns, or concerns around the breach of privacy law, or the revelation of 'information about the client that could form the basis of discriminatory practices such as the refusal of credit facilities'.[10]

[9] 2017 supplement, para 14

[10] 2017 guidance, para 110

This consequently leads to the collection of additional information. As the FATF 2017 guidance notes, 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]

This dynamic comes up on numerous occasions in the draft guidance.
On two-factor authentication (p186) the FATF considers this a 'minimum'. It's worth noting recent abuses and the use of this data for advertising by Twitter and Facebook.[12] While making it a 'minimum' seems progressive from a security perspective, ensuring limited processing is key to enhancing security and confidence in what we would agree are essential security processes. Therefore, a strong and enforceable legal framework with ongoing monitoring and transparency is essential.

The FATF shows much interest in 'ownership and inherence authenticators (p183). It notes particularly device fingerprinting, 'biomechanial biometrics' and behavioural biometric patterns. These must be placed in the larger context of being used for profiling and data mining,[13] and not, in fact, 'developed and

---

[11] 2017 guidance, paragraph 67.

[12] https://privacyinternational.org/news-analysis/3251/use-2fa-information-commercial-purposes-unacceptable and https://privacyinternational.org/report/3025/facebook-must-explain-what-its-doing-your-phone-number-update

[13] See for instance the research from Princeton University's Center for Information Technology Policy, with one instance covered here: https://www.theregister.co.uk/2018/01/17/html5_online_tracking/

deployed primarily for anti-fraud purposes'. In turn, we should be considering what happens in a future when these mechanisms are abused and rejected by people and institutions, and the FATF remains the institution promoting such techniques. From a security model standpoint, it is also highly problematic that additional data may be included into banking processes, e.g. a banking app could having access to 'individual's email or text message patterns, file access log, mobile phone usage, and geolocation patterns' (p175, quoting an MIT piece) would be a breaking of mobile security best practices of limiting the data and permissions to which an app has access.[14]

We could therefore imagine a day where browsers start preventing device fingerprinting, and the interpretation of FATF guidance is that banks would not let people use browsers unless fingerprinting is possible; in turn, banks will start using apps instead, and requiring the use of these apps, that then use third party development kits that also allow both first and third parties to have access to greater levels of data on bank customers opening them up for new forms of profiling, targeting, and discrimination. And all of these essential transactions will be occurring on devices with weak security models, for fear of introducing security and privacy safeguards that would reduce fraud but break mobile banking.

Already the draft guidance takes a stance on digital ID enabling transaction monitoring (p109). This is later expanded that the use of digital ID may allow information that is collected for anti-fraud purposes to be used for AML/CFT purposes. At the moment there is softer language that:

"to the extent such information is accessible to them, regulated entities should consider using authentication data to enable the detection of systematic misuse of digital IDs, including compromised, stolen or sold digital IDs. This

[14] see our study on mobile apps with extensive data-sharing problems with Facebook https://privacyinternational.org/campaigns/investigating-apps-interactions-facebook-android and particularly for low-cost tech https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price--have-pay

information could be considered in identifying and determining whether to report suspicious activities. One possible benefit of the federated identity model is that identity fraud detection can be shared across a network of identity providers and relying parties."

This will likely be interpreted by identity providers and regulated entities alike that they should be monitoring digital ID systems on an ongoing basis for AML/CFT, and across the identity ecosystem, thereby further shaping the digital ID market.

## CONCLUSION

It's because of the importance of financial processes in peoples' lives that we are concerned by the standards set by the FATF in the digital sphere, that could play a disproportionate role in the establishment of new technological infrastructure. While the FATF's early stands on identity led, perhaps unintentionally, to the deployment of extensive, expensive, and intrusive identity systems across the world, we cannot let that happen again without more deliberation. Otherwise we will look back again in twenty years' time and notice that these recommendations swayed the development of the future in a way that is incompatible with rights, freedom, and dignity.

## INFORMATION ON PI

Privacy International

www.privacyinternational.org

Privacy International (PI) campaigns for legal and technological solutions to protect people and their data from exploitation. Founded in 1990 and based in London, PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom.

Our vision is that freedom and privacy will be the foundations of tomorrow's societies. This means that people are enabled by technology to explore their identities, speak their minds, and live with dignity. They will be free from exploitation and in control of their lives.

Privacy International, a registered UK charity (no. 1147471), registered with Companies House of England and Wales (no. 04354366), and is governed by a Board of Trustees. Our registered offices are 62 Britton Street, London, EC1M 5UY, Great Britain.

Contact: Gus Hosein, Executive Director, gus@privacyinternational.org

**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**