Comments to the Financial Action Task Force on the March 2021 Draft updated Guidance for a risk-based approach to virtual assets and VASPs

April 19, 2021

To whom it may concern:

Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using open blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

We welcome this opportunity to comment on the FATF's draft guidance. For clarity we have included a table of contents outlining our three major concerns with respect to the draft guidance as well as an addendum with a list of specific textual ambiguities and suggested edits.

Thank you for your consideration,

Peter Van Valkenburgh
Director of Research
Coin Center

Table of Contents

Introduction

FATF is strongly focused on preventing the abuse of our financial system by terrorists and criminals. That said, FATF's recommendations can have severe impacts on persons who are neither terrorists or criminals: persons who are developing innovative new technologies, persons who have been left behind by the global financial system, and persons who rightly wish to defend their personal privacy from ever encroaching, big-tech-enabled surveillance.

It is incumbent upon FATF to balance the good of stopping terror and crime against the harms inherent in unintentionally criminalizing benign conduct; de-banking, de-platforming, and censoring already disadvantaged populations; and robbing the innocent of reasonable and treaty-based and/or constitutionally mandated privacy protections and rights to free expression.

The recent "Draft updated Guidance for a risk-based approach to virtual assets and VASPs" (hereinafter draft guidance) does not adequately strike that balance because of three miscalibrations:

1. The "expansive" new interpretation of the definition of "virtual asset service providers" (VASPs) will erode certainty and the rule of law with regard to who amongst various virtual asset actors are and are not obliged entities. It will also extend mass warrantless surveillance obligations well beyond what has been the norm in the world of traditional finance, and it will effectively deny many persons their treaty-based and/or constitutional rights to free expression. Moreover, it will undermine existing and as-of-yet incomplete efforts by member states to extend reasonable AML regulation to centralized platforms by forcing competent authorities to instead engage in the Sisyphean task of pursuing mere software developers and other non-custodial network participants.
2. The proposal that VASPs prohibit or severely restrict peer-to-peer and privacy-enhanced transactions will deny innocent persons access to private and censorship-resistant payments, will stifle promising innovations that could otherwise benefit our shared struggle against crime and terrorism, and will only push criminals and terrorists a further level underground, allowing them to carry out their nepharious plans unhidered and with even less visibility to law enforcement.
3. The inclusion of VASP-to-non-VASP transactions within the scope of "travel rule" obligations (in particular the demand for customer counterparty information) misinterprets existing travel rule obligations within member states, causing confusion and necessitating redrafting, and—worse—would be incompatible with foundational statements of human rights to privacy and a warrant requirement for searches and seizures. For example, such a policy could not become law in the United States under

the Fourth Amendment and similarly would conflict with treaty obligations in jurisdictions party to the European Convention on Human Rights (ECHR) and International Covenant on Civil and Political Rights (ICCPR).

We realize that this is an extensive list of critiques rooted in significant policy and human rights concerns. We do not intend to suggest that FATF has intentionally tread into these weighty issue areas. It is likely that many of these concerns are merely the result of imprecise drafting and could easily be addressed in a subsequent draft. While making the above policy arguments, our comment will remain very specific about which passages in the draft offend, and how they may be corrected should FATF members be amenable. As always, we thank the FATF for the opportunity to contribute to an important policy discussion.

An "expansive" definition of VASP

In the draft guidance, FATF announces a "conscious choice" to abandon the existing reasonable and justiciable definition of VASP in favor of an "expansive" reinterpretation of the category.[1] This choice represents a significant and unwise departure from FATF's previous guidance in 2019. The breadth and vagueness of this new interpretation is also irreconcilable with any sensible reading of the FATF Recommendations themselves as well as the laws of member states that have pioneered VASP regulation up to this point.

In brief, should this radically new expansive approach be adopted, it will undo the meaningful progress FATF and member states have made in crafting a reasonable AML regime for virtual assets since 2013. The proposed expansive definition of VASP cannot be reconciled with the rule of law and basic human rights to privacy and free expression. FATF should redraft the guidance such that actual independent control over customer virtual assets remains the determinative standard for qualifying as a VASP. It is a justiciable standard and it is the existing standard in several member nations.[2]

To assist the FATF we have compiled in the addendum to this comment an exhaustive list of paragraphs from the draft guidance that appear to go beyond an independent control standard or, generally, takes an expansive approach. We also include suggested changes in that list. While it is a lengthy list that may appear to advocate a major revision and substantive policy

[1] "Draft updated Guidance for a risk-based approach to virtual assets and VASPs," Financial Action Task Force, FATF Draft Guidance, March 2021, https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf, page 29, paragraph 76.
[2] "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," Financial Crimes Enforcement Network, U.S. Department of the Treasury, FinCEN Guidance FIN-2019-G001, May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf.

change, we note that several sections of the draft FATF guidance already present a somewhat contradictory interpretation of VASP that is not expansive and does not include persons without independent control:

1. Paragraph 54 where "conduct[ing] a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another." is identified as a determinative of who is covered as transferring VASP.[3]
2. Paragraph 47 where it is proposed that "A DApp itself is not a VASP".[4]
3. Paragraph 68 where it is proposed that "A person that develops or sells either a software application or a VA platform may therefore not constitute a VASP when solely developing or selling the application or platform."[5]
4. The entirety of paragraph 69, which clearly excludes hardware and non-custodial wallet manufacturers and developers, internet service providers, and miners and validators.[6]
5. Box 4 which excludes "validators" of stablecoin transactions and manufactures and software providers of hardware and "unhosted" wallets.[7]

We are unsure whether these seemingly contradictory statements are the remnants of a previous, now half-abandoned narrow approach to the definition of VASP or if the new "expansive" language listed in the addendum is, somehow, intended to be compatible with these statements. On the face, they do not appear compatible. For example, how can the following statements be reconciled?

> Box 4: *Developers are VASPs if they deploy programs whose functions fall under the definition of VASP and they deploy those programs as a business on behalf of customers.*[8]

And

> Paragraph 68: *A person that develops or sells either a software application or a VA platform may therefore not constitute a VASP when solely developing or selling the application or platform.*[9]

If, after all, the developer is allowed to "develop" and "sell" her "VA platform" without being a VASP (according to Paragraph 68) then how is she not also "deploy[ing] those programs as a business on behalf of customers," an activity that would make her a VASP under Box 4? Persons selling software have customers.

---

[3] *Supra* note 1, page 22.
[4] *Id*., page 21.
[5] *Id*., page 26.
[6] *Id*., page 26.
[7] *Id*., page 28.
[8] *Ibid*.
[9] *Id*., page 26.

Indeed, most DApp developers do not sell their software but rather release it, *gratis*, under open source licenses. While these persons seem surely to be outside of the definition of VASP as interpreted in the Paragraph 68 statement above, might they still be VASPs under the Box 4 standard? What is even meant in Box 4 by "as a business on behalf of customers?" FATF has been clear that it intends the definition to be "expansive"[10] and elsewhere mentions that so-called "owner/operator(s) of the DApp"[11] and persons who "conduct() business development for a DApp"[12] are included. DApps do not have owners as traditionally understood because they are merely software published to a permissionless blockchain. Does FATF intend the "owner" to be the person with intellectual property rights to that software? Or persons with trademark rights to certain brands or marks that have become associated with that software? Generally none of these persons have any actual control over the assets of DApp users. Moreover, in the case of open source software with multiple contributors, these persons could number in the thousands and encompass original developers who have long since left the software development effort altogether.

To the extent FATF is speaking of persons who do, however, have control of an administrative key that would, in fact, afford them independent control over customer assets, we do not disagree that these persons may be VASPs, and we offer suggestions in the addendum for how to more clearly offer guidance on that policy. However, to the extent FATF is speaking merely of persons who do "business development," which in the software community generally means technical service and education with regard to integrating software into other applications, or mere software development and publication itself, we do not agree with FATF and note that such an expansive treatment would swallow the sensible exclusion provided at Paragraph 68. Additionally, such a policy would likely conflict with the constitutional rights of software developers and users in the United States, as well as basic human rights of developers the world over as understood in the ECHR and ICCPR, as we will argue later in the comment.[13]

Similarly contradictory, observe the stated definition of transfer that is reiterated at Paragraph 53:

> Paragraph 53: *conduct[ing] a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another.*[14]

---

[10] For instance, "The FATF takes an expansive view of the definitions of VA and VASP and considers most arrangements currently in operation, even if they self-categorize as P2P platforms, may have at least some party involved at some stage of the product's development and launch that constitutes a VASP." *Id.*, page 29.
[11] *Id.*, page 23.
[12] *Ibid*.
[13] *Infra* "Effectively denies many persons basic human rights to free expression" section.
[14] *Supra* note 1, page 22.

With the newly drafted guidance at Paragraph 55:

> Paragraph 55: *Service providers who cannot complete transactions without a key held by another party are not disqualified from falling under the definition of a VASP.*[15]

We should be able to agree that, depending on the particular multi-sig arrangement, someone will have independent control: either the virtual asset owner herself (*e.g.* in a 2-of-3 multi-sig arrangement where the owner has 2 keys and a service provider has 1 key) or the service provider (*e.g.* in a 2-of-3: owner 1 key, service provider 2 keys) or both (*e.g.* 1-of-2: owner and service provider each have 1 key). This person or persons will ultimately be able to conduct a transaction moving the asset from one address to another as per Paragraph 53, and because Paragraph 53 rightly does not include persons conducting transactions on their own behalf within the definition of VASP only the second and third examples above involve VASPs under the transfer limb of the VASP definition.

This is the result under the justiciable "independent control" standard that we advocate: only the second and third of those examples would be VASPs because it is only in those cases where some service provider has the actual ability to transact on behalf of another. Paragraph 55, however, confuses this justiciable standard. If a person "cannot complete [a] transaction" (paragraph 55) then she cannot "conduct a transaction that moves a virtual asset from one address to another" (paragraph 53), and yet paragraph 55 goes on to say that she is nonetheless "not disqualified from falling under the definition." How can this person then still be a VASP under Paragraph 55 if she does not meet the stated definition of a transferring VASP in Paragraph 53? Is she doing one of the other activities aside from transferring? If so, why is this "not disqualified" language found in the "transferring" section of the guidance? If "all dogs are VASPs" then guidance explaining that "not being a dog does not disqualify you from being a VASP" is not particularly helpful within the context of guidance on being a dog.

If the intent of Paragraph 55 is to cover service providers who partner with other service providers to secure customer virtual assets (*e.g.* a 2-of-3 multi-sig: service provider A has one key and contracts with service provider B to store the second key, customer has the third key) then Paragraph 55 is unnecessary and remains confusing because the service provider was already included by Paragraph 53: she *does* have independent control because she will have some contractual promise (explicit or implicit) from her fellow service provider to cooperate and transact irrespective of any keys held by the customer. To the extent that this interpretation is unclear, we suggest in the addendum to this comment an edit to Paragraph 55.

If, on the other hand, the customer is the final determinant of a transaction because of keys she herself has secured (perhaps with various service providers that she has chosen and who are not

[15] *Ibid*.

in any contractual relationship with each other), then none of the "service providers" involved will have independent control because none of them can "conduct a transaction." In this case, these service providers are not providing financial services, they are safekeeping a string of numbers that cannot, on its own, generate a valid virtual asset transaction. Indeed these service providers may merely be generic "cloud" data storage providers or even, in the case of hardware wallets, physical self-storage device makers. In this arrangement, the customer is acting as her own financial services provider, she may be using non-financial service providers for data or physical storage but she remains the only person in the arrangement with actual control of any assets.

Again, the clearer statement of what constitutes a transaction and, therefore, "control" for purposes of the definition of VASP is the stated definition: "conduct[ing] a transaction on behalf of another natural or legal person that moves a virtual asset from one virtual asset address or account to another." This standard alone is sufficient to create a justiciable definition of VASP and should not be muddied with the several seemingly contradictory statements about "multi-sig" described above.

As a final example of these contradictions, observe

> Paragraph 75: *Automating a process that has been designed to provide covered services does not relieve the controlling party of obligations.*[16]

And, again,

> Paragraph 68: *A person that develops or sells either a software application or a VA platform (i.e., a software developer) may therefore not constitute a VASP when solely developing or selling the application or platform.*[17]

The only method of truly "automating" a financial service of which we are aware is by creating software that, when run by several persons on a peer-to-peer network, allows individuals to perform the service peer-to-peer without a trusted intermediary. If "automating" and "developing software" are, indeed, overlapping categories, then these paragraphs are contradictory. "Developing software" and "automating" are both valid ways of describing, for example, what the pseudonymous creator of the Bitcoin network did by publishing the Bitcoin core protocol software.[18] By releasing that software and encouraging persons across the world

[16] *Id.*, page 29.
[17] *Id.*, page 26.
[18] Satoshi Nakamoto, "Bitcoin v0.1 released," The Cryptography Mailing List, January 8, 2009, https://www.metzdowd.com/pipermail/cryptography/2009-January/014994.html.

to run it on their internet connected computers,[19] Satoshi Nakamoti made a previously intermediated financial service—electronically transferring something of value—into an automated process. Under the proposed draft guidance Satoshi, along with anyone else who has ever published cryptocurrency software is "not relieve[d] of obligations" and presumably then, may be a VASP. This is, of course, absurd as well as contradictory to the second statement exempting software developers in the guidance listed above.

If, on the other hand, all that is meant by Paragraph 75 is that "automating a process" while one continues to have independent control over customer virtual assets does not disqualify the person with independent control from being a VASP, then we do not disagree, but we do not understand what is meant by "automating a process" and we do not think the guidance is improved by complicating what would otherwise be a clear statement that maintaining independent control of customer virtual assets satisfies the definition of being a VASP. If all cats are VASPs then nothing is gained by offering guidance that cats who drink milk are VASPs.

Vague statements, internal contradictions, and potential absurdities such as these are not conducive to either better surveillance of the financial system or of a justiciable rule that would avoid unintended consequences or human rights violations. For this reason, as described in the suggested changes in the addendum, we ask FATF to simplify its guidance on the VASP definition such that actual independent control over customer virtual assets remains the determinative standard. It is a justiciable standard and it is the existing standard in several member states.[20] Failure to do so would invite the following serious policy consequences (intended or no).

Erodes certainty and the rule of law

The decision to classify a category of entities as a VASP is not a matter to be taken lightly. When one is classified as a VASP, one is ordered to engage in warrantless mass surveillance of her fellow citizens and ordered to systematically deny and shun persons who cannot or choose not to identify themselves sufficiently. Further, the nature of the obligations that a VASP must undertake may preclude that person from freely engaging in certain actions that are their human right and, in many FATF member states, their constitutional rights as well.[21]

The gravity of that classification means that calibrating its scope is something that democratically elected governments should do very carefully when they make law; should they fail to account for and honor the rights of their citizens, at the very least the process is

[19] "If you can keep a node running that accepts incoming connections, you'll really be helping the network a lot." *Ibid*.
[20] *Supra* note 2.
[21] *Infra* "Effectively denies many persons basic human rights to free expression" section.

transparent and the participants are accountable for their failings at the ballot box or in the courts of justice. FATF is not obligated by law to be transparent nor are FATF members elected by any democratic process.[22] It is all the more important, therefore, that FATF tread carefully when basic human rights are at stake. Indeed, the International Covenant on Civil and Political Rights (ICCPR), the European Convention on Human Rights (ECHR), and many national basic laws (including the U.S. Constitution), each require that laws enabling surveillance be narrowly specified and detail the specific circumstances and conditions under which a citizen will no longer be entitled to privacy (*e.g.* a court-issued warrant or where there is reasonable suspicion of criminal wrongdoing) . Simply saying that a particular surveillance regime is enacted through law is not sufficient; the law must be precisely drafted and narrowly tailored to accommodate the right of individuals.

Under the ECHR any interference with the privacy of citizens must be "in accordance with the law."[23] At a minimum this means that the interference must be based in some domestic statute. It also, however, refers to the quality of the law. As Sweedish legal scholar Mark Klamberg aptly summarizes, the law "must be (1) accessible to the person concerned, who must, moreover, be able to (2) foresee its consequences for him or her, and (3) compatible with the rule of law… [It must be] formulated with sufficient precision to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to measures of surveillance."[24] As we saw with the contradictions and vague standards described in the previous section, the current draft guidance does not describe *foreseeable* consequences and does not give citizens an adequate indication of which circumstances will trigger surveillance.

Similarly, as the UN Committee on Human Rights (OHCHR) has found with respect to Article 17 of the ICCPR,

> The expression 'arbitrary interference' can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, *reasonable in the particular circumstances*…

[22] "Who we are," Financial Action Task Force, accessed April 16, 2021, https://www.fatf-gafi.org/about/whoweare/#d.en.11232.
[23] European Convention on Human Rights, "Right to respect for private and family life," Article 8, European Court of Human Rights, Council of Europe, September 3, 1953, https://www.echr.coe.int/documents/convention_eng.pdf.
[24] Benjamin Wittes, "Mark Klamberg on EU Metadata Collection," *Lawfare*, September 29, 2013, https://www.lawfareblog.com/mark-klamberg-eu-metadata-collection.

> Even with regard to interferences that conform to the Covenant, relevant legislation *must specify in detail the precise circumstances* in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and *on a case-by-case basis*.
>
> Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited [emphases added].[25]

The recent guidance, to the extent it is intended to influence the creation of laws in states party to the ICCPR, is not exempted from this call for specificity, and yet the current draft does not exhibit a careful or narrowly specified approach.

Several passages describe a "conscious choice"[26] by the FATF to craft "expansive" definitions[27] such that "very few VA arrangements will form and operate without a VASP involved at some stage."[28] In no uncertain terms this language calls for an expansive approach to surveillance that is neither "case-by-case" as the UNCHR requires under the ICCPR,[29] nor "formulated with sufficient precision to give citizens adequate notice" as the ECHR demands. The consequences of a vague and expansive definition that carries with it warrantless surveillance obligations and severe criminal penalties for non-compliance is either mass surveillance (everyone who participates in these computer networks must spy on and report about their peers) or else mass criminalization (everyone who joins these free and open networks without seeking prior government approval is a felon).[30] An "expansive" approach to these highly consequential definitions is not compatible with the rule of law and individual rights in a free society.

With that said, the horrors of terrorism and the continued specter of international crime may warrant some level of financial surveillance. Rather than choosing an "expansive" approach, a clear line should instead be drawn between those whose actions reasonably justify an obligation to surveil their fellow citizens and those whose actions do not. This would not be an "expansive" definition. It may be a broad category of persons but it should not be vaguely specified and indiscriminately flexible. To allow flexibility is to invite uncertainty: too many private entities may argue that the vague standard does not encompass them and too many government officials may use the discretion afforded them by an "expansive" definition to

---

[25] United Nations Human Rights Committee, "General Comment 16," Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc HRI/GEN/1/Rev.1 (Twenty-third session, 1988) http://hrlibrary.umn.edu/gencomm/hrcom16.htm.
[26] *Supra* note 1, paragraph 76, page 29.
[27] *Id.*, paragraph 75.
[28] *Id.*, paragraph 76.
[29] *Supra* note 25.
[30] 18 USC 1960.

harass and oppress the innocent but politically or socioeconomically unfavored. It is therefore the duty of FATF to carefully craft a reasonable and informative definition of VASP that precisely encompasses only those whose actions justify surveillance obligations and clearly excludes persons engaged in no such actions.

What then is a clear and justiciable line for that definition? The answer is straightforward: *the actual assumption of independent control over another person's virtual assets (whether to safekeep or transmit those assets) on their behalf*. This is the standard articulated in the previous draft guidance,[31] it is the standard found within any reasonable reading of the existing recommendations,[32] and it is the standard in the existing laws and regulations of several key FATF member states.[33]

Extends mass warrantless surveillance obligations beyond the norm

It is not sufficient for the line between obliged parties and non-obliged parties to only be well defined, or—as we have said—justiciable. The gravity of surveillance obligations and the collateral effect of surveillance on human flourishing demands that the line also describe a reasonably limited sector of human action. We could make a very clear and justiciable line by simply saying that all adults over 18 are obliged to register with financial intelligence units (FIUs) and report the details of their transactions. This, obviously, would be beyond the pale of reasonable protections for civil liberties and would be so difficult to enforce consistently that it would generate the same rule of law difficulties as a vague standard. FATF must therefore be mindful both of the vagueness of the law but also its breadth.[34]

---

[31] "Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers," Financial Action Task Force, June 2019, http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.

[32] "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations," Financial Action Task Force, October 2020, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

[33] *Supra* note 2.

[34] *See, generally*: Kiel Brennan-Marquez, "Extremely Broad Laws," 61 *Arizona Law Review* 641 (2019): pgs. 642-666, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3205783. Brennan-Marquez cleverly personifies these two species of troublesome law with appropriate literary embodiments. A vague law, he writes, is Kafkaesque: legal pitfalls hide 'round every corner and the benefit of the law—certainty—is denied through obfuscation and doubt, a perpetual fear of its uncertain application. A broad law is Orwellian: the demands of the law are clear but those demands are so extensive as to entirely curtail human flourishing. It is the terror and immobility of living under a police state, Orwell's Oceania, rather than the absurdity and self-imposed immobility of wasting one's whole life waiting before a fearsomely guarded gate that was, in Kafka's "Before the Law," deceptively unlocked and free for passage all along.

No evidence has been presented of rampant criminality on these networks that is in any way more significant than existing criminality within the legacy financial system.[35] Accordingly, the breadth of obligations for these networks should be the same. FATF appears to agree on this score. When describing "limb iii" of the VASP definition, "transferring," the new draft guidance says:

> The limb is conceptually similar to what Recommendation 14 on money and value transfer services (MVTS) covers for traditional financial assets. An example of a service covered by (iii) includes the function of facilitating or allowing users to send VAs to other individuals, as in a personal remittance payment, payment for non- financial goods or services, or payment of wages. A provider offering such a service will likely be a VASP.[36]

We agree that finding analogs with traditional financial services (*i.e.* taking a functional approach) is useful in determining who amongst various virtual asset actors should be an obliged entity. If it walks like an MVTS and quacks like an MVTS, it is likely an MVTS. That said, the above statement from the draft guidance characterizing MVTS is deceptively broad and does not, in fact, accurately describe the range of persons currently treated as MVTS under Recommendation 14 or under the laws of member states. The established FATF Recommendations define MVTS as:

> *Money or value transfer services (MVTS)* refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs.[37]

There are two key elements that trigger classification as an MVTS in that definition: "acceptance" and "payment." A person is acting as an MVTS when she both "accepts" some value from another person and "pays" a corresponding value to the same person (at another location) or to another person. Note how this definition creates a clear and justiciable line: you are only doing MVTS if you actually accept something of value from someone else and pay a corresponding value. The precision of this definition means that there is less need for clumsy carve-outs to address unintended consequences. For example, we know we would not want this definition to apply to a lunch clerk who merely accepts payment in order to sell sandwiches.

---

[35] Aly Madhavji and Alek Tan, "Comparing Money Laundering With Cryptocurrencies and Fiat," *CoinTelegraph*, July 30, 2020, https://cointelegraph.com/news/comparing-money-laundering-with-cryptocurrencies-and-fiat.
[36] *Supra* note 1, page 23.
[37] *Supra* note 31.

The definition does a good job of not including her: she may accept cash but she does not "pay" a corresponding sum of cash, and to argue that the sandwich is a corresponding sum of value would be insane.

Now let's look again at the characterization of MVTS in the draft guidance:

> The limb is conceptually similar to what Recommendation 14 on money and value transfer services (MVTS) covers for traditional financial assets. An example of a service covered by (iii) includes the function of facilitating or allowing users to send VAs to other individuals, as in a personal remittance payment, payment for non- financial goods or services, or payment of wages. A provider offering such a service will likely be a VASP.[38]

Here there is only one key element that triggers classification as a VASP: "the function of facilitating or allowing users to send [value] to other individuals." First, we have no idea what is meant by "the function" in this language. "Performing the function of feeding the cat" is, so far as we are aware, the same as simply "feeding the cat." So we are left with merely a "facilitating or allowing" standard.

In the context of MVTS would a "facilitating or allowing" standard be justiciable and reasonably narrow? After all, the draft says these definitions are meant to be similar. Let's check. Does the U.S. Mint "facilitate" or "allow" persons to send value to each other? Absolutely, by printing cash and minting coins, the U.S. Mint facilitates the activities of any person who uses these items to send value. Does a telephone company "allow" persons to send value? Absolutely, by connecting persons over the phone such that they can agree to terms of a value transfer, the telephone company "facilitates" and "allows" a transfer to take place. We could, in theory, obligate the telephone company to only connect persons who are not criminals or terrorists, but such a broad obligation might be difficult for the telephone company to faithfully carry out, and several innocent people might no longer be able to easily use telephones. Similarly, could we obligate the U.S. Mint to identify the names and physical addresses of every person who uses their currency to commit illicit transactions? We could attempt such an obligation, but the friction it would place on all cash transactions globally and the tremendous resources the Mint would have to consume in order to survey each cash exchange might grind the world economy to a halt.

We know that FATF has no intention to include telephone companies or mints within the scope of MVTS obligations. We merely ask for parity in the virtual asset space. There are several persons who perform the analog to MVTS in the cryptocurrency space (they both "accept" and "pay" assets on behalf of their customer) and they should be regulated accordingly. There are

[38] *Supra* note 1, page 23, paragraph 55.

also several persons who perform the analog to a telephone or minting service in the virtual asset space. They do not "accept" and "pay," but rather they write software, validate the cryptography in transaction messages, relay those messages without discretion, or even hold some number of cryptographic keys but without the ability to ever transact on behalf of a customer, indeed they generally don't have customers. Like a telephone company or a mint, these people undoubtedly "facilitate" and "allow" persons to transact using virtual assets, and they could in theory be obligated to block those transactions just as a mint or telephone company could be so obligated. But the primary result of such obligations would not be less crime, it would be a near total disruption of virtual asset networks. This is why the draft language is inappropriate, it characterizes the category of obliged persons in an absurdly broad way. "The function of facilitating or allowing users to send VAs" is not a faithful analog to the MVTS definition. A faithful analog would be an "independent control" standard as was previously the policy of FATF[39] and as is the policy in several member states.[40]

Before it is binding on persons or businesses, any FATF recommendation must first be enacted into law by a member state. In some member states, a constitution may preclude certain policy choices from ever being enacted as law. In the U.S. at least, this constitutional limitation would be a strong barrier to enacting any law or regulation that creates surveillance obligations on persons who do not independently control the virtual assets of another. Coin Center has published an extensive report on the constitutional infirmities inherent in a hypothetical application of financial surveillance laws to non-custodial persons within the virtual asset ecosystem.[41] In that report we describe how,

> The [U.S. Constitution's] Fourth Amendment prohibits warrantless search and seizure of information over which persons have a reasonable expectation of privacy.[42] Existing [Bank Secrecy Act] recordkeeping and reporting requirements are constitutional despite collecting large amounts of information without warrants because bank customers are said to lose their reasonable expectation of privacy when they voluntarily hand this information over to a third party in furtherance of a legitimate business purpose of that third party.[43] If users do not voluntarily hand this information to a third party because no third party is necessary to accomplish their transactions or exchanges, then they logically retain a reasonable expectation of privacy over their personal records and a warrant would be required for law enforcement to obtain those records. Users cannot be

[39] *Supra* note 31, paragraph 41, page 16.
[40] *Supra* note 2.
[41] Peter Van Valkenburgh, "Electronic Cash, Decentralized Exchange, and the Constitution," *Coin Center*, March 2019, https://www.coincenter.org/electronic-cash-decentralized-exchange-and-the-constitution/.
[42] *Id.*, at note 23.
[43] *Id.*, at note 24.

> forced to record and report their lawful activities without violating the 4th Amendment's warrant requirement.[44]
>
> Similarly, financial institutions can be forced to record and retain customer data because their customers willingly hand that data over to them and because that data are essential to their conduct of legitimate business purposes.[45] Developers of electronic cash and decentralized exchange software have no legitimate business purpose for collecting that data and users do not volunteer that information to developers when they use their software tools. Indeed, a software developer will likely be even less aware of who is using their tools than the author of a book would know who has bought a copy and read it. Deputizing software developers to collect this information as a prerequisite to publishing their software tools would be unconstitutional under the Fourth Amendment because it would constitute a warrantless seizure of information over which users have a reasonable expectation of privacy.

This argument extends both to persons who develop cryptocurrency or DApp software,[46] as well participants in multi-signature payment channels like the Lightning Network.[47] None of these persons have either a legitimate business purpose to collect otherwise private user data and neither do the users of these software and network tools expect to voluntarily provide that data to any other person. Indeed the users and the maintainers of the networks never meet, they do not even have the opportunity to discover with whom they could potentially exchange personal data.[48] These tools work based on cryptographic signatures, game theory, and computer networks rather than personal interactions, contractual agreements, or customer guarantees.

One can no more "know" or have a legal relationship with a member of the Lightning Network when one sends payments across that network than one could "know" or have a legal relationship with the person who maintains undersea cables when using the internet to communicate with someone overseas.[49] None of the providers of these services ever has independent control over the virtual assets of the network users and therefore participants have no need for recourse to the courts in the event of malfeasance. Should a particular node's actions cause a transaction to fail, the user can simply try again to make her transaction and some other node on the network will eventually create the throughput that the other node

---

[44] *Id.*, at note 25.
[45] *Id.*, at note 26.
[46] So long as they do not also have or retain independent control over DApp users' virtual assets.
[47] Elizabeth Stark, "Lightning Network," *Coin Center*, September 15, 2016, https://www.coincenter.org/education/key-concepts/lightning-network/.
[48] Lightning network transactions are instead routed through channels that are passively connected by participating nodes. One can explore the network of Lightning nodes using an explorer such as: https://explorer.acinq.co/.
[49] *Id.*

failed to provide. This is similar to the nature of Bitcoin miners: if one miner fails to add a user's transaction to a block then some other miner will pick up the slack if there is a competitive fee attached to the transaction. Miners can never "steal" or otherwise redirect user transactions because they never have independent control over those virtual assets.[50] This is also, again, similar to the nature of packet switching networks[51] for internet data: a user's internet traffic data often fails to reach the destination through one particular node, but the network of nodes picks up the slack. Personal data such as a legal name and physical address is not only irrelevant to the creation and usage of these network technologies, it would pose a severe information security and storage challenge to everyone involved.

The expansive standard suggested by the recent draft guidance would not be dissimilar to mandating that everyone must send a text message to a financial crimes regulator whenever they make a cash transaction. Indeed it would be even more onerous than that, it would be as if every person maintaining a node on the internet must get the name and physical address of every person whose packets of internet data are relayed by their node. The impracticality of that requirement is not a mere inconvenience, it speaks directly to the Fourth Amendment argument: if such information collection and reporting was mandated it would not be collected for any legitimate business purpose by third parties and customers would not otherwise voluntarily provide it. As such, that information retains the protections offered by the Fourth Amendment.[52] It cannot be searched or seized by the government, or by a financial institution acting on behalf of the government, unless a judge has granted a valid warrant.[53] Warrants must be specific in the U.S.[54] and, accordingly, no bulk suspicionless surveillance requirements would be constitutional.

Nor is this an uniquely American requirement. International and European treaties on human rights also require that searches and seizures of personal information be permitted only under specific conditions. Indiscriminate bulk surveillance is simply not permitted.

As the UN Secretary-General has found in the context of the ICCPR and electronic mass surveillance,

> By permitting bulk access to all digital communications traffic, this technology eradicates the possibility of any individualized proportionality analysis. It permits

[50] Peter Van Valkenburgh, "What is Bitcoin mining, and why is it necessary?" *Coin Center*, December 15, 2014, https://www.coincenter.org/education/advanced-topics/mining/.
[51] Lawrence G. Roberts, "The Evolution of Packet Switching," *IEEE Invited Paper*, November 1978, https://web.archive.org/web/20160324033133/http://www.packet.cc/files/ev-packet-sw.html.
[52] *Supra* note 41.
[53] *Id.*
[54] *Id.*

> intrusion on private communications without independent (or any) prior authorization based on suspicion directed at a particular individual or organization.[55]
>
> Article 17 of the Covenant provides that any interference with private communications must be prescribed by law, and must be a necessary and proportionate means of achieving a legitimate public policy objective… Merely to assert — without particularization — that mass surveillance technology can contribute to the suppression and prosecution of acts of terrorism does not provide an adequate human rights law justification for its use. The fact that something is technically feasible, and that it may sometimes yield useful intelligence, does not by itself mean that it is either reasonable or lawful (in terms of international or domestic law)
>
> The suggestion that users have voluntarily forfeited their right to privacy is plainly unwarranted. It is a general principle of international human rights law that individuals can be regarded as having given up a protected human right only through an express and unequivocal waiver, voluntarily given on an informed basis. In the modern digital world, merely using the Internet as a means of private communication cannot conceivably constitute an informed waiver of the right to privacy under article 17 of the Covenant.[56]

The same is true, we argue, with regard to mere use of a peer-to-peer virtual asset network even if that network involves some other participants who "do business development," "automation," or who participate in some other non-custodial way. Users do, indeed, waive these rights against mass financial surveillance when they willingly and knowingly agree to hand their money or virtual assets over to a third-party bank or custodial VASP for safekeeping, but they do no such thing when they merely participate in a peer-to-peer transfer during which no other party actually controls their funds on their behalf.

A mandate ordering open-source developers to include surveillance tools in their software will, by necessity, compromise the privacy of every software user irrespective of circumstance. A mandate that any participant in peer-to-peer networks for virtual assets shall run only approved surveillance-compatible software would be similarly indiscriminate. Such an approach is not and cannot be compatible with case-by-case decision making, and fundamental privacy rights.

---

[55] "Promotion and protection of human rights and fundamental freedoms while countering terrorism," United Nations, General Assembly Report, A/69/397, September 23, 2014, https://theintercept.com/document/2014/10/15/un-report-human-rights-terrorism/.
[56] *Ibid*.

Effectively denies many persons basic human rights to free expression

As FATF notes in the draft guidance, some DApps and decentralized stablecoin arrangements have "central" participants who reatian "some measure of involvement" by performing various functions: "business development," "automation," "creating and launching an asset," or "holding an administrative 'key.'" Let us set aside "holding an administrative key"; as stated earlier, Coin Center agrees with the FATF that possession of an administrative key that offers independent control over customer assets legally justifies the imposition of AML obligations. The other listed activities, however, should not be sufficient to justify classification as a VASP and the attendant mass surveillance obligations.

Law enforcement and AML regulators should be gratified that several popular DApps retain central participants and that those participants do not feel the need to hide their identities. While these persons do not and should not meet the definition of a VASP; they remain valuable partners in investigations and a resource for policymakers seeking insight into any potential criminal usage of their respective software tools. Treating these people as VASPs would not further deepen that cooperation, however. Instead it would force these developers to compromise their tools and, likely, their fundamental beliefs in privacy-protecting and censorship-resistant virtual asset technologies. Rather than comply, it is likely that many would instead cease publishing their DApp software and cease performing these "central" functions within their DApp's ecosystem. If the DApp is already instantiated on a permissionless blockchain, it would nonetheless continue to function without them.[57] Additionally, other developers would likely continue publishing DApp software anonymously.

Every DApp and decentralized stablecoin arrangement that has been released to date could have been made and released anonymously by persons hiding their identity. These tools are simply software code published to permissionless blockchain networks where users can freely find and interact with them. The only true precondition is access to an Internet connection. If FATF classified DApp "business development" or DApp "automation" as virtual asset service

[57] Take, for example, the smart contract that powers EtherDelta decentralized exchanges. EtherDelta's original creator Zachary Coburn was charged with operating an unregistered securities exchange and he settled with the Securities and Exchange Commission and consented to a cease-and-desist order. *See:* "Order Instituting Cease-and-Desist Proceedings Pursuant to Section 21(c) of the Securities Exchange Act of 1934: In the Matter of Zachary Coburn," Release No. 84553 (Nov. 8, 2018), *available at* https://www.sec.gov/litigation/admin/2018/34-84553.pdf. Nonetheless, the Ether Delta smart contract that, in fact, enables persons to trade tokens and, potentially, unregistered securities has continued to operate beyond that settlement and remains freely accessible to Ethereum users to this day. *See:* "Contract 0x8d12A197cB00D4747a1fe03395095ce2A5CC6819," *Etherscan Block Explorer*, available at https://etherscan.io/address/0x8d12a197cb00d4747a1fe03395095ce2a5cc6819#code. Short of outlawing access to the thousands of copies of the Ethereum blockchain that exist on the Internet and are where this "automation" of financial services resides, there is no way to stop persons from seeing it, and, should they wish, using it.

provision, and if member states then demanded that these developers become licensed and report on the activities of their users, many would simply develop DApp software and refuse to do "business development" or "automation." Instead, they would quietly publish that DApp software across the internet without performing any other "central" activities. To the extent states might seek to restrict such publication, the DApp source code itself could be shared as works of visual art, encoded in music, or silk-screened onto t-shirts. This is exactly what encryption software advocates did when U.S. authorities attempted to restrict publication of encryption source code in the name of weapons export control laws.[58] As a policy, those restrictions were a dramatic failure and were ultimately found unconstitutional in court.[59]

In restricting otherwise free software development, FATF would not be responsibly directing member states to engage in sensible policy to stop money laundering. Instead it would be directing member states to dedicate scarce resources to an endless game of whack-a-mole: chasing down nameless and faceless publishers of computer code who share their software on every and any communications platform on the internet or even in the physical world. It is a recipe for failure. It would also necessitate crushing censorship and a severe curtailment of constitutional and human rights to free expression.

Specifically, any mandate that required open source DApp software developers to build KYC or other compliance tools into their software would run afoul of Article 19 of the ICCPR, Article 10 of the ECHR, as well as the U.S. Constitution's First Amendment prohibition on compelled speech.

Open-source computer code shared over the internet is directly intended to convey the scientific and engineering ideas of a given project to other developers, including current collaborators, potential future collaborators, researchers, and the general public who may wish to use these tools and seek assurances of their correct operation, which can only be achieved through publicity and transparency. If digital tools derived from this science and engineering will be employed to, for example, organize social behavior on the internet, then their source code certainly holds at least as much social and political significance in the 21st century as a schematic of a steam engine or a blueprint for an amphitheater would have held in previous ages.

---

[58] Adam Back, "Munitions T-shirt," accessed June 6, 2019, http://www.cypherspace.org/adam/uk-shirt.html.

[59] Ronald J. Stay, "Cryptic Controversy: U.S. GovernmentRestrictions on Cryptography Exports and thePlight of Philip Zimmermann," 13 *Georgia State University Law Review* 1 (February 1997): pgs. 581-604, https://readingroom.law.gsu.edu/gsulr/vol13/iss2/14.

Indeed, the "unfettered interchange of ideas"[60] found in computer code is the primary motivation behind open-source software development as a practice. Rather than cloister one's software project within the developer staff of a single corporation by enforcing copyrights, trade secrets, and other restrictions on dissemination through a proprietary software model, open-source software development principles eschew copyrights and restrictive licenses, push for better ways to clearly and publicly display source code for review, and seek to solicit the widest possible audience in order to increase the odds that a member of that audience will catch errors that would otherwise go undetected or find opportunities for innovation that would otherwise have been missed. This ethos is long-established and well-captured in developer Eric Raymond's landmark 1997 essay *The Cathedral and the Bazaar*.[61] All major electronic cash and decentralized exchange software projects rigorously adhere to this open-source model of development. Canonical changes to that software are only made after an exhaustive round of public sharing and discussion of the code itself.[62]

---

[60] *Roth v. United States*, 354 U.S. 476 (1957) https://supreme.justia.com/cases/federal/us/354/476/.

[61] In the essay, Raymond explains several emergent rules in the open source developer community: "Every good work of software starts by scratching a developer's personal itch." The majority of developers in an open-source project are motivated primarily because they want to use the product they are making. They aren't under contract to build something for someone else; they have a personal need and they are addressing it. This leads to greater motivation and it brings intimate personal knowledge about the problem to bear. "Good programmers know what to write. Great ones know what to rewrite (and reuse)." When development happens in the open, redundancy can be avoided, a division and specialization of knowledge and expertise achieved, and troublesome, complicated, or redundant code identified and simplified. "When you lose interest in a program, your last duty to it is to hand it off to a competent successor." People come and go within an open-source project depending on their interests and expertise. No one gets stuck working on projects they no longer care about and fresh minds appear to offer different perspectives on longstanding problems or new avenues for development. "Treating your users as co-developers is your least-hassle route to rapid code improvement and effective debugging." Many of the people who use the open-source code will also be able to identify and flag issues, and may even be able to offer solutions. The line between a consumer and a producer of open-source software blurs because production happens transparently in full view of the public and participation in production is available to all. "Given a large enough beta-tester and co-developer base, almost every problem will be characterized quickly and the fix obvious to someone." This has come to be known as Linus's Law after Linus Torvalds, the original creator and longtime principal developer of Linux. When development is not open, all developers may share a certain blind spot or fail to notice a certain error. Wider development amongst sophisticated users with idiosyncratic perspectives increases the likelihood that bugs are discovered and addressed, thus making open-source software more resilient and secure. *See*: Eric S. Raymond, *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Cambridge, MA: O'Reilly, 1999.

[62] *See*, *e.g.*: the so-called block size debate among the Bitcoin community. *For an overview, see*: Aaron van Wirdum, "Segregated Witness, Part 3: How a Soft Fork Might Establish a Block-Size Truce (or Not)," *Bitcoin Magazine* (Dec. 29, 2015) https://bitcoinmagazine.com/articles/segregated-witness-part-how-a-soft-fork-might-establish-a-block-size-truce-or-not-1451423607/.

With certainty we can say that thousands of persons independently work to publish open-source cryptoasset software, DApps, and other decentralized financial tools.[63] It is impossible to say with certainty how many more persons—perhaps tens of thousands, hundreds of thousands, or millions—subsequently relay and share that published software through various online and offline communication channels. A law granting the FATF member states discretion to decide which versions of this software can and cannot be published and shared within and across their borders would be difficult (to say the least) to implement and enforce.

If a regulator was to mandate that all open-source software must include surveillance backdoors, the mandate would effectively order developers to rewrite existing software libraries in order to include code that implements the backdoor. Each of these open-source software libraries typically has several hundred authors and there are several hundred if not several thousand different libraries for various versions of Bitcoin and other cryptoasset wallets and protocols. Whose responsibility would it be to comply with these orders? Are all of the developers who have previously contributed to the software obligated to help write the backdoor code? Or would it only be developers living in the FATF member state who are obligated? Should the onus rest with some new developer who can be persuaded to add a backdoor in a derivative version of the code? Can you force someone to engage in creative and difficult software design against their will? We can speculate that many privacy- and civil-liberties-focused developers would simply choose not to write that code.

Even assuming that some versions of cryptoasset software do end up having backdoors because of an order from a FATF member state, how can the regulator ensure that the several other versions of cryptoasset software lacking backdoors are not published and shared amongst its citizens? The regulator would have to ban the communication of a broad class of information: any cryptoasset software that does not comply cannot be transmitted on the internet or shared through printed books within their borders. As mentioned earlier, in order to illustrate the difficulty of such a ban in the encryption context, advocates have previously gone so far as to silk-screen cryptography protocols onto t-shirts.[64] Would a FATF member state need to outlaw certain illicit apparel if need be?

Practicality aside, a law empowering regulators to whitelist the publication of certain open-source cryptoasset software partnered with a blanket ban on the publication and distribution of non-compliant software would violate Article 19 of the ICCPR, Article 10 of the ECHR, as well as the First Amendment rights of U.S. Citizens. Both the ICCPR and ECHR hold that persons should have "the freedom to hold opinions and to receive and impart information

[63] *See* the repositories for the Bitcoin and Ethereum reference clients: https://github.com/bitcoin and https://github.com/ethereum.
[64] Adam Back, "Munitions T-shirt," accessed June 6, 2019, http://www.cypherspace.org/adam/uk-shirt.html.

and ideas without interference by public authority and regardless of frontiers."[65] Both conventions find that the exercise of these rights carries "special duties and responsibilities" that justify a limited range of restrictions on speech.[66] These restrictions must be made through law rather than at the discretion of public authorities. These restrictions must be formulated with "sufficient precision to enable an individual to regulate his or her conduct accordingly and [] must be made accessible to the public."[67] Any scheme empowering a regulator with discretion to whitelist select versions of cryptoasset software would, by design, fail to provide sufficient precision and perspicuity to enable citizens to regulate their own conduct.

Nor would a blanket ban on cryptoasset software publication withstand constitutional and human rights scrutiny. Specifically in the context of software and the internet, UN General Comment No. 34 to Article 19 of the ICCPR finds that "generic bans on the operation of certain sites and systems" are not compatible with the ICCPR.[68]

General Comment No. 34 also finds that it would be incompatible with the ICCPR "to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information. Nor is it generally appropriate to include in the remit of such laws such categories of information as those relating to the commercial sector, banking and scientific progress."[69] At a fundamental level, crypoasset software is, itself, scientific and engineering research. Moreover, while crimes committed by persons using cryptoasset software to, for example, move illicit funds could, in extreme hypotheticals, harm national security, the software itself does not. Additionally, several persons utilize these tools in their fight to protect human rights.[70]

The General Comment finds that restrictions must be proportional to the threat they seek to address and should be "the least intrusive instrument amongst those which might achieve their protective function."[71] As described in the first half of this comment letter, a narrow and justiciable "independent control" standard for qualifying persons as VASPs reasonably addresses the threats of money laundering without stifling the free exchange of ideas and the

---

[65] *See*: Council of Europe, "European Convention on Human Rights," Article 10, *European Court of Human Rights* (Sep. 21, 1971) https://www.echr.coe.int/Documents/Convention_ENG.pdf; United Nations, "International Covenant on Civil and Political Rights," Article 17, *UN Office of the High Commissioner for Human Rights* (Dec. 16, 1966) https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
[66] *Id*.
[67] *Id*.
[68] United Nations, "General Comment No. 34," *Human Rights Committee*, CCPR/C/GC/34 (Sep. 12, 2011) https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.
[69] *Id*.
[70] *Infra* "Denies innocent persons access to private and censorship-resistant payments" section
[71] *Id*.

free publication of software. Banning the publication of software and other purpose-neutral technologies is, self-evidently, not the least-intrusive approach to stopping people from using those tools to launder money.

A primary motivation behind the development of this technology is the global decline of cash transactions (which are inherently private and lacking in intermediaries).[72] This decline has been matched with the rise of powerful, private financial technology intermediaries that can systematically surveil their users and arbitrarily exclude them from economic life simply by closing their account. Such private surveillance and arbitrary power, argue electronic cash advocates, contravenes the rule of law. In nation states with weaker human rights guarantees, governments can and are actively partnering with these intermediaries to obtain greater control over their populations.[73] If cash disappears, advocates claim, only electronic cash and decentralized exchange technologies can serve as a safety valve against imminent payments-technology-enforced totalitarianism.[74]

One does not need to personally subscribe to these views in order to grasp the gravity of the human rights issues at hand. It is sufficient to believe that virtual asset software developers earnestly hold these views and publish their software to express them (rather than for some other, cynical purpose). If this much is true, then bans on software publication wade dangerously into the territory of stifling a vibrant and consequential debate. Such a policy would violate the fundamental and unqualified right of persons to hold and form opinions as found in Article 19 of the ICCPR, Article 10 of the ECHR, and the First Amendment of the U.S. Constitution.

FATF members may argue that the current draft does not place restrictions on the authorship and publication of software, citing the exemptions at Paragraph 68. Again, several newly proposed paragraphs appear to contradict and swallow the exemption at Paragraph 68. Further, to the the extent that "business development" and "automation" can be separated from DApp software development, and to the extent that surveillance obligations can be limited to persons doing these activities, it is entirely likely that several persons will create identical DApps not subject to surveillance obligations merely by quietly publishing software alone and eschewing any public facing activities that could trigger obligations. At that point, law enforcement will have fewer cooperative parties with which to partner in these ecosystems, and fewer windows into the illicit flows of funds over these networks. Thereafter, FATF may believe it has few remaining options apart from classifying mere software authors as VASPs and subjecting them

[72] Jerry Brito, "The Case for Electronic Cash," *Coin Center*, February 2019, https://www.coincenter.org/the-case-for-electronic-cash/.
[73] *Id.*
[74] *Id*.

to surveillance obligations. That would be a last resort that is, as we have described, incompatible with the rule of law and basic human rights.

Will burden competent authorities with a Sisyphean task

While FATF does not appear to acknowledge the many rule of law or human rights difficulties inherent in an expansive definition of VASP, it does mention the burden that enforcing a vague standard may place on the governments of member states:

> The FATF recognises however that such an approach can bring practical challenges to competent authorities in identifying which entities are VASPs and defining their regulatory perimeter.

FATF, however, is severely understating the problem. Authorities in several member states are already far behind implementation of the June 2019 update to the FATF Guidance for a Risk-Based Approach to Virtual Currencies.[75] In many regions, and as described in the Fifth and most recent Money Laundering Directive from the European Parliament, purely virtual aset to virtual asset transactions on centralized platforms are, to this date, outside of the regulatory perimeter.[76] This is an extraordinary state of affairs given that, for example, in the U.S. these transactions have been subject to Bank Secrecy Act requirements since at least 2013.[77]

Non-surveilled centralized international exchanges remain by far the single largest issue with respect to virtual assets and money laundry.[78] FATF's new "expansive" standard will complicate commonsense efforts to bring ordinary centralized virtual asset exchanges into basic compliance with existing AML obligations. As described above, chasing down mere software developers or making abstract determinations about persons having "control" despite not having "unilateral control" will only serve to slow and complicate the already delayed roll-out of non-controversial AML obligations in many member nations.

Unenforceable and seemingly contradictory standards will confuse what would otherwise be a straightforward policy initiative and may erode the credibility and authority of the FATF within the policy-forming organs of member states. Inevitable and highly visible failures to meet

---

[75] *Supra* note 31.
[76] "Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU," May 30, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843.
[77] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," Financial Crimes Enforcement Network, U.S. Department of the Treasury, FinCEN Guidance FIN-2013-G001, March 18, 2013, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
[78] "270 Service Deposit Addresses Drive 55% of Money Laundering in Cryptocurrency," *Chainalysis*, February 11, 2021, https://blog.chainalysis.com/reports/cryptocurrency-money-laundering-2021.

unrealistic goals will only serve to embolden criminals who will perceive an erosion of the rule of law, and repeated conflict will weaken collaborative efforts between industry and regulators.

FATF's solution to these difficulties is to provide a vague rubric for competent authorities:

> When there is a need to assess a particular entity to determine whether it is a VASP or evaluate a business model where VASP status is unclear, a few general questions can help guide the answer. Among these would be who profits from the use of the service or asset, who established and can change the rules, who can make decisions affecting operations, who generated and drove the creation and launch of a product or service, who possesses and controls the data on its operations, and who could shut down the product or service. Individual situations will vary and this list offers only some examples.

As we have argued throughout, none of these questions have clear answers. Bitcoin itself has had countless persons who "generated and drove the creation and launch" of the network. Even Coin Center would struggle with performing an accurate historical accounting of contributions to the Bitcoin protocol. "Establishing … the rules" is a process that is indistinguishable from software development as it is within protocol software that all rules are encoded. The set of persons who can "change the rules" within a protocol includes at least every person who voluntarily chooses to run one or another version of protocol software on his or her internet connected computer. Take for example the split between Ether and Ether Classic over the rules of the DAO smart contract.[79] Or the split between Bitcoin and Bitcoin Cash over the rules for the block size.[80] In each case it was the decisions of every network member to either update or not update their software that led to rule changes.[81]

The number of nodes on these networks is always fluctuating but at last look Coin Center can identify at least 9,733 Bitcoin nodes spread across at least 95 countries[82] and 5,136 Ethereum nodes spread across 67 countries.[83] These are, however, only the "listening" nodes on their respective networks, nodes that have been configured to accept incoming connections from other nodes. A listening node can help new nodes on the network to find peers and to download the blockchain; maintaining a listing node is like providing a public service to the network at large. Non-listening node maintainers refuse to provide this service by refusing new connections from new peers, but they can still compile full copies of the network's blockchain

[79] Paul Vigna, "The Great Digital-Currency Debate: 'New' Ethereum Vs. Ethereum 'Classic'," *Wall Street Journal*, August 1, 2016, https://www.wsj.com/articles/BL-MBB-52061.
[80] Jonathan Bier, *The Blocksize War: The battle over who controls Bitcoin's protocol rules*, BitMEX Research (2021): https://blog.bitmex.com/the-blocksize-war/.
[81] *Ibid*.
[82] *See*: https://bitnodes.io/.
[83] *See*: https://ethernodes.org/.

and can still mine, as well as send, receive and validate transaction messages and blocks; they are, however, more difficult to track. Estimates of total bitcoin nodes, including non-listening nodes, currently hover around 100,000.[84] How is a competent authority to determine whether any of these nodes are presently contemplating "chang[ing] the rules" of any decentralized protocol within their borders? What good is it to address the actions of those persons when rules will certainly be changed or not changed by other nodes irrespective of the actions of nodes within their borders? And aren't these nodes excluded from obligations under the FATF's own standards in Paragraph 69 as miners/validators? It is counterproductive to reasonable AML policy to burden already overwhelmed AML authorities with such confusing and metaphysical inquiries. Coin Center urges FATF to simplify the rubric at Paragraph 77 to a justiciable "independent control" standard.

Prohibiting VASPs from making peer-to-peer and privacy-enhanced transactions

At various points FATF encourages member states to consider the prohibition of so-called peer-to-peer and anonymity-enhanced transactions as a means of mitigating risk.[85] Prohibitions such as these will not mitigate risks, they will only decrease law enforcement visibility into virtual asset networks by fragmenting these networks between surveilled VASP-to-VASP transactions and entirely untraceable transactions between non-VASPs. This strategy would increase AML/CFT risks while simultaneously harming innocent individuals who may have legitimate reasons for engaging in private and peer-to-peer transactions.[86] A prohibitory policy would also discourage promising digital identity innovations that could otherwise present longer term solutions to the problem of terrorist and criminal usage of the financial system.[87]

Rather than pursuing a prohibitory strategy, or some other vaguely specified risk-based strategy, FATF should simply direct member states to direct obliged VASPs to treat any transaction not involving another VASP as if it were a physical cash transaction. Financial Institutions already have various strategies in place for dealing with the risks presented by cash transactions and in several jurisdictions these transactions, when above a certain threshold, trigger a report to financial intelligence units (a currency transaction report).[88]

---

[84] Colin Harper, "Are You Running a Bitcoin Node?" *CoinDesk*, January 29, 2021, https://www.coindesk.com/are-you-running-a-bitcoin-node.
[85] *Supra* note 1, paragraphs 91(c), 94, 95.
[86] *Infra* "Denies innocent persons access to private and censorship-resistant payments" section
[87] *Infra* "Stifles promising innovations that could benefit our shared struggle against crime" section
[88] 31 CFR §1010.410(b) and (c).

Bitcoin and other cryptocurrencies are best analogized to electronic cash,[89] and therefore applying these same reporting requirements to cryptocurrency deposits and withdrawals has, at least, the benefit of technological neutrality and parity with longstanding obligations placed on traditional financial institutions. We discourage FATF from attempting to make case-by-case determinations about virtual assets (*e.g.* classifying some as "anonymity-enhanced" cryptocurrencies). All virtual assets apart from those that are centrally controlled will likely become "anonymity-enhanced" as development continues. Some already have this feature inherent in the basic operation of their protocol,[90] others have or will have additional "layers" and/or transaction types developed to enable these privacy protections.[91] The fact that some blockchains currently reveal details of personal transactions unencrypted to the public at large is widely regarded as a bug in current implementations and it will no doubt be corrected through community open-source development in short order. Rather than take a soon-to-be-obsolete technology-specific approach, FATF should simply advise member states to treat all transactions that are not bookended by a VASP as they would physical transactions in cash.

Currency transaction reports[92] dealing with virtual assets need not share invasive personal information about transaction participants. The single discrete fact conveyed by a traditional currency transaction report is that a particular customer has removed a particular amount of value from the otherwise surveilled financial system into the unsupervised realm of person-to-person transactions involving bearer instruments. Upon receiving that report a responsible FIU can make the determination whether to seek additional information from the reporting institution if, and only if, reasonable suspicion and a legal process warrants that further scrutiny. Therefore, FATF should not advise member states to require invasive information such as blockchain transaction IDs, sending or receiving blockchain addresses, or other identifying information apart from customer names within these reports. That information will be available to law enforcement should a warrant or other formal legal process deem its collection necessary to an investigation.

A prohibitory approach to peer-to-peer and privacy-enhanced transactions, on the other hand, would have the following deleterious public policy consequences.

---

[89] *Supra* note 72.
[90] Andrea O'Sullivan, "What are mixers and 'privacy coins'?" *Coin Center*, July 7, 2020, https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/.
[91] *Id*.
[92] *Supra* note 88.

Denies innocent persons access to private and censorship-resistant payments

To start, there is nothing inherently nefarious about wanting to engage in a person-to-person transaction rather than an intermediated transaction. For the vast majority of human history all transactions were person-to-person and left no central record of transaction details. And yet society was not lawless.

Indeed, it is the advent of fully surveilled, fully intermediated transactions that represents a worrying departure from long standing practice and cryptocurrencies may, indeed, simply be a sensible reversion to the mean.[93] Fully surveilled and intermediated transactions are deeply problematic in states that do not have strong democratic institutions and commitments to individual rights. If a person's financial transactions can be fully surveilled and her access to financial transactions fully blocked, then she is at the mercy of the state and would have little ability to resist a totalitarian or unjust regime. This has recently been the case in two regions of note: Nigeria and Belarus.

In Belarus a non-profit organization, BYSOL, has found that traditional intermediated payment methods are unable or unwilling to accommodate transactions fulfilling their mission and has therefore turned to peer-to-peer bitcoin transactions as an alternative.[94] BYSOL's mission is to support pro-democracy protesters and persons or families who have been victimized for engaging in pro-democracy advocacy. BYSOL's peer-to-peer Bitcoin donations directly "provide assistance [for] funds for medical, sports and cultural solidarity, strike committees at enterprises, families of political prisoners," and vocational retraining for persons who have been fired from their jobs for "participation in peaceful actions and strikes."[95] As of December 2020, BYSOL has raised and paid over $3 million in support of these initiatives.[96]

This past year in Nigeria, Feminist Coalition, an equal rights advocacy organization, became a key group accepting donations to support emergent anti-police brutality protestors under the banner #EndSARS.[97] Feminist Coalition quickly found that their donations were being blocked or otherwise censored by banks and online payments providers at the direction of the government. Faced with no real alternative, Feminist Coalition began accepting Bitcoin donations. As of October 2020, when Feminist Coaltion ceased taking donations because a

[93] *Supra* note 72.
[94] Anna Baydakova, "Belarus Nonprofit Helps Protestors With Bitcoin Grants," *CoinDesk*, September 9, 2020, https://www.coindesk.com/belarus-dissidents-bitcoin.
[95] *See*: https://bysol.org/en/faq/.
[96] *Ibid*.
[97] Yomi Kazeem, "How bitcoin powered the largest Nigerian protests in a generation," *Quartz*, October 26, 2020, https://qz.com/africa/1922466/how-bitcoin-powered-nigerias-endsars-protests/.

government curfew "effectively ended physical protests in Lagos," almost 40% of the $387,000 raised had come from these peer-to-peer bitcoin transactions.[98]

These two examples are merely the most recent and illustrative cases of the good that peer-to-peer bitcoin transactions can do in supporting democracy and a free civil society. To prohibit such transactions is to play directly into the hands of dictators and totalitarian regimes.

Stifles promising innovations that could benefit our shared struggle against crime

FATF acknowledges that "strong digital identity solutions" are needed in order to mitigating the risks posed by illicit activities and fraud.[99] FATF's own policy to prohibit or limit VASP transactions with non-VASP wallets, however, directly encumbers the emergence of these important identity solutions.

A reliable decentralized identity solution only works if the person who is proving her identity has actual control over cryptographic keys related to blockchain-based identity assets and can exert that control by making transactions from her "self-hosted" wallet to the blockchain itself. If this hypothetical person was forced to rely on an intermediary "hosted" wallet provider for identity credentials, then the identity system would suffer from all of the same cybersecurity vulnerabilities of existing centralized identity providers (*e.g.* if the service provider is compromised, so too are the identities of every person who uses the service). This has been the case time and time again for enterprise identity tools (see *e.g.* an estimated 1.2 million compromised accounts in January 2020 alone[100]), government systems (see *e.g.* the U.S. Office of Personnel Management hack[101]), and individual consumers (see *e.g.* the 2017 Equifax hack[102]). There is no blockchain solution to this problem that would not involve users possessing several discrete "unhosted" wallets as parts of a multi-factor identification protocol.

---

[98] *Id.*
[99] *Supra* note 1, page 13, paragraph 31.
[100] Zak Doffman, "Microsoft Confirms 'Really, Really High' Hacking Risk For Millions Of Users: Here's What You Do Now," *Forbes*, March 7, 2020, https://www.forbes.com/sites/zakdoffman/2020/03/07/microsoft-confirms-really-really-high-hacking-threat-for-millions-of-users-heres-what-you-do-now/?sh=282959f49b66.
[101] Ellen Nakashima, "Hacks of OPM databases compromised 22.1 million people, federal authorities say," *Washington Post*, July 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.
[102] AnnaMaria Andiotis and Ezequiel Minaya, "Equifax Reports Data Breach Possibly Affecting 143 Million U.S. Consumers," *Wall Street Journal*, September 8, 2017, https://www.wsj.com/articles/equifax-reports-data-breach-possibly-impacting-143-million-u-s-consumers-1504819765.

For example, a wallet on the user's phone signs cryptographic transactions to the blockchain proving her identity and allowing her to enter a building. A wallet on the phone of the building's administrator can revoke or reprovision the user's phone with keys by making a similar transaction to the blockchain. A paper wallet in the user's house contains backup keys that can, again, be used to revoke the authority of the user's phone if she loses it. The only way that such a system improves upon existing identity tools is by removing the single point of failure and spreading keys across self-hosted wallets held by the user and by others individually. Consolidate those keys into one or even a few wallets controlled by service providers on behalf of several customers and the issue of hacks and single-points of failure returns. Blockchains do very little to prevent hacks aside from providing a reliable public ledger such that individuals can hold and transact with their own credentials; if you remove the self-custody of credentials aspect of "blockchain technology" all you have left is an absurdly overbuilt database tool and one vulnerable provider holding all of the keys.

Identity may have seemingly little to do with cryptocurrency blockchains and therefore appear irrelevant to AML policies. It is important to keep in mind, however, that permissionless blockchain networks are by far the most reliable networks from an information security standpoint. The costs of rewriting or fraudulently altering the Bitcoin blockchain are astronomical as compared with any centralized or quasi-centralized database tool. It is for this reason that companies like Microsoft have invested heavily in building enterprise identity systems on top of the Bitcoin blockchain.[103] Similarly, several decentralized identity tools have emerged on top of Ethereum.[104] With *any* identity tool built on top of a public permissionless blockchain there will be a need for users to make tiny payments with their self-hosted wallet in order to pay fees inherent in writing information to the distributed ledger. This means that these self-hosted wallets, even if used primarily for innovative identity solutions, will be effectively identical to self-hosted wallets used for investing or moving money. In all cases the software is the same and the cryptographic addresses are indistinguishable. Therefore, any restriction that places barriers needlessly on transactions to self hosted wallets would inevitably also burden decentralized identity tools.

[103] Pamela Dingle, "ION - Booting up the network," Microsoft Tech Community, June 10, 2020, https://techcommunity.microsoft.com/t5/identity-standards-blog/ion-booting-up-the-network/ba-p/1441552

[104] *See, for example*: "Azimuth," Urbit Development Docs, https://urbit.org/docs/glossary/azimuth/.

Pushes criminals and terrorists a further level underground

Cryptocurrency software has become ubiquitous;[105] it will be available to people regardless of their motives (good or bad) and irrespective of regulation. If FATF took steps to isolate regulated financial institutions from software-enabled peer-to-peer or anonymity enhanced transactions it would, certainly, stop civil society organizations like BYSOL or Femenist Coalition from effectively fundraising, and it would, without doubt, hinder enterprise software providers like Microsoft's efforts to build truly robust decentralized identity tools. What it would not do, however, is further reduce the already minimal[106] criminal usage of these technologies.

Criminals and terrorists would likely celebrate the segmentation of these networks into regulated and unregulated halves. The fact that cryptocurrency transactions regularly flow into and out of regulated exchanges is the number one reason these networks are not particularly useful for criminals. Eventually, a criminal will slip up and some combination of blockchain analyses or need to cash out at a liquid (and therefore likely regulated) institution will be their undoing. Steps to limit the free exchange of cryptocurrencies between regulated and unregulated wallets will, all things being equal, further shield criminal usage from law enforcement's view.

Take, for example, the so-called Swiss Rule[107] approach to wallet identification. Under the rule, regulated exchanges are only allowed to send and receive transactions from wallets that are verifiably identified, usually by the exchange's customer themself. If a criminal who has yet to arouse suspicion is using a Swiss Rule compliant exchange, she will simply choose to send her cryptocurrency to a self-hosted wallet address that she herself controls and has identified to the exchange. If her end goal is to send cryptocurrency to a sanctioned address or some criminal counterpart she can now simply send a transaction from her own address, perhaps through a mixing transaction, to the sanctioned address. Depending on the quality of the mixing, this transaction may not reveal her illicit activities to the exchange even if they continue to monitor the blockchain. From the exchange's perspective an ordinary customer has simply moved her cryptocurrency to an address she controlled and then made other subsequent transactions with

---

[105] For example, an estimated 100,000 persons run a version of the bitcoin protocol software around the world. The software is available for free and without the need to obtain a license at various locations across the internet including Github repositories, websites, and peer-to-peer file download networks.
[106] Aly Madhavji and Alek Tan, "Comparing Money Laundering With Cryptocurrencies and Fiat," *CoinTelegraph*, July 30, 2020, https://cointelegraph.com/news/comparing-money-laundering-with-cryptocurrencies-and-fiat.
[107] "Payments on the blockchain," Swiss Financial Market Supervisory Authority, FINMA Guidance 02/2019, August 26, 2019, https://finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20190826-finma-aufsichtsmitteilung-02-2019.pdf?la=en.

those funds going forward. This situation is in no way better than one where the exchange's customer was able to ask the exchange to pay some other address directly. The added hop to the customer's self-hosted wallet, if it does anything at all, merely serves to add noise to the exchange's ability to root out a signal of illicit use.

The inclusion of VASP-to-Non-VASP transactions within the scope of "travel rule"

At various sections of the guidance, FATF states that Recommendation 16 should and does apply to transactions between a VASP and a non-VASP. However, FATF's own Recommendation 16 is not currently defined such that it would, under any reasonable legal interpretation, apply to these types of transactions. Nor is the "travel rule" in jurisdictions like the U.S. defined to apply to transactions between a VASP and a non-VASP. Moreover, any mandate under Recommendation 16 to use the travel rule to force the collection information about a customer's counterparty that is not otherwise already revealed by the customer would be a grave violation of the privacy rights of that counterparty. FATF should alter these sections of the draft guidance, listed in the addendum, and, instead, urge VASPs to treat such transactions as they would cash deposits or withdrawals.

Misinterprets existing travel rule obligations

Recommendation 16 as currently drafted applies to "wire transfers and related messages."[108] The interpretive note to Recommendation 16 defines wire transfers accordingly:

> Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.[109]

Note that while the term applies to transactions irrespective of whether the originator and beneficiary are the same person, it is clearly defined to only include transactions that are both (a) "carried out … through a financial institution" in order to (b) make funds "available to a beneficiary person *at a beneficiary financial institution.*" As defined, wire transfer would not include a transaction carried out through a financial institution to pay a person directly rather than to make funds "available to the beneficiary person at a beneficiary financial institution." Nor would the term include a transaction that made funds "available to the beneficiary person at a beneficiary financial institution" if the transaction was not also "carried out … through a

[108] *Supra* note 31, page 78.
[109] *Id.*, page 83.

financial institution." In other words, the definition of wire transfer clearly imagines that the transaction will be bookended by one or more financial institutions.

This is, no doubt, already the case with cash withdrawals and deposits: if a customer pays her financial institution with cash or has her financial institution pay her with cash there is, of course, no wire transfer involved. This is commonly and rightly understood as a different sort of transaction: a cash withdrawal or deposit. These types of transactions rightly trigger different (and in some cases more) surveillance obligations.[110] Virtual asset transactions, when they are not bookended by one or more financial institutions should, also, be understood as- and regulated as cash withdrawals or deposits.

Nothing in the current Interpretive Note to Recommendation 15 (explaining application of FATF recommendations to new technologies) would suggest any diversion from this commonsense reading of Recommendation 16 in the context of virtual assets. INR 15 simply says that under Recommendation 16:

> Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities."

Understanding that Recommendation 16 describes records to be kept for transactions book-ended by financial institutions, a VASP could assume from the above that they must therefore comply as a traditional financial institution would comply whenever a transaction is book-ended by VASPs. Nothing, however, indicates that they must somehow treat transactions with non-VASPs as wire transfers.

Nor did the previous draft guidance conflict with this commonsense interpretation, emphases added:

> In accordance with the functional approach of the FATF Recommendations, the requirements relating to wire transfers and related messages under Recommendation 16 apply to all providers of such services, including VASPs that provide services or engage in activities, such as VA transfers, that are ***functionally analogous to wire transfers.***
>
> Consequently, the requirements of ***Recommendation 16 should apply to VASPs whenever their transactions***, whether in fiat currency or VA, ***involve***: (a) a traditional

[110] For example, a cash withdrawal over 10,000 will trigger a currency transaction report to FIUs irrespective of whether the transaction is suspicious. A wire transfer over 10,000 will not trigger any automatic report to any FIUs unless the transaction is suspicious.

> wire transfer, or (b) ***a VA transfer or other related message operation between a VASP and another obliged entity.***

A transaction that is not bookended by VASPs is not functionally analogous to a wire transfer. Wire transfers only ever happen between financial institutions. To the extent such transactions have a functional analog, it would be to a cash deposit or withdrawal, or to a check being endorsed from one person to another person (irrespective of whether either person is a customer of the checkbook-issuing bank).

FATF should not apply the wire transfer rule to these transactions because it is illogical, and it certainly cannot apply the rule through guidance that conflicts with a plain reading of the existing recommendations and associated interpretive notes.

Additionally, the travel rule requires that the two sides of a wire transfer share and exchange the required customer information. This information is what "travels" in the so-called "travel rule." Obviously FATF does not intend to have VASPs send sensitive customer information to non-VASPs in the case of transactions not bookended by a VASP. Rather than simply clarifying what is already obvious in the Recommendations, the current draft guidance simply states that VASPs should not send information in those "special" cases.

> The FATF does not expect that VASPs and FIs, when originating a VA transfer, to submit the required information to individuals who are not obliged entities.

Effectively, the guidance is confusingly arguing that a rule that does not appear to fit a particular transaction at all should, nonetheless, be applied, but that only the parts that make sense (VASPs record information) should apply and not the parts that do not make sense (information travels with the wire). This flexible interpretation is, yet again, incompatible with basic rule of law principles that binding policies should be clearly articulated and applied generally.

We will not analyze every member state's particular implementation of Recommendation 16, but we will briefly look at the US rule (where the term "travel rule" first emerged). In the opening paragraph of FinCEN's own travel rule advisory, the rule is described accordingly:

> A Bank Secrecy Act (BSA) rule—often called the "Travel" rule—requires all financial institutions to pass on certain information to the next financial institution, **in certain funds transmittals involving *more than one* financial institution**.[111]

[111] "Funds 'Travel' Regulations: Questions & Answers," Financial Crimes Enforcement Network, U.S. Department of the Treasury, FinCEn Advisory Issue 7, January 1997, https://www.fincen.gov/sites/default/files/advisory/advissu7.pdf

The Bank Secrecy Act implementing regulations themselves define "funds transfers" as "a series of transactions, beginning with the originator's payment order" and "completed by acceptance by the beneficiary's bank."[112] Meanwhile "payment order" is defined as "an instruction… to a receiving bank."[113] Once again, these definitions apply to transactions bookended by financial institutions or VASPs. They do not make sense in the context of transactions between a VASP and a non-VASP. An individual making a Bitcoin transaction from her self-hosted wallet to an address at a VASP is *not* sending "an instruction… to a receiving bank," she is making a transaction message to be received by miners or validators on the Bitcoin network. Similarly, a VASP sending a transaction to a self-hosted wallet address is not undertaking a "series of transactions … completed by acceptance by the beneficiary's bank." The regrettably strange term "unhosted" wallet (self-hosted is more illustrative) self-evidently describes a situation where the recipient has no bank accepting anything on her behalf, she is instead accepting the virtual asset directly.

Is incompatible with privacy rights and gravely endangers innocent persons

Application of the travel rule to transactions not bookended by VASPs inherently demands that VASPs obtain private information about persons who are not their customers. In traditional travel rule compliance, no information is recorded or exchanged except information about the customers of the financial institutions in question. These customers will have already voluntarily supplied this information with their bank as a necessity of obtaining banking services. A person who is holding her own virtual assets, however, will have never voluntarily consented to any personal information being recorded or exchanged by financial institutions with which she has never even interacted. To subject these persons to invasive mass surveillance without them ever having affirmatively waived their rights to privacy violates the ICCPR[114] and the ECHR[115] as well as the Fourth Amendment to the U.S. Constitution.[116]

The personal information sought is, indeed, very private. Merely linking a name to a physical address can compromise the privacy of the resident. Linking a Bitcoin payment address (which may indicate personal wealth)[117] to a name and physical address is extremely destructive of the owner's privacy and indeed may jeopardize her safety as she may become a target of a

[112] 31 CFR 1010.
[113] *Id.*
[114] *Supra* note 23.
[115] *Supra* note 25.
[116] *Supra* note 41.
[117] For example, one can observe the holdings of Bitcoin addresses by examining the block chain. In this early ledger entry, we can see that this address, believed to be controlled by the creator of Bitcoin Satoshi Nakamoto, contains 50 BTC, which is worth over $1 million today: https://www.blockchain.com/btc/block/000000006a625f06636b8bb6ac7b960a8d03705d1ace08b1a19da3fdcc99ddbd.

kidnapping or extortion plot.[118] Additionally, there is a high likelihood that several of these records will be reported to FIUs in SARs and CTRs and through subpoenas. U.S. FIU FinCEN's records have recently been the subject of extensive leaks[119] and a recent hack of a Financial Institution in India has compromised the "ID scans, passports, emails, phone numbers and addresses of nearly 100 million persons."[120] If FIUs were to maintain extensive records of Bitcoin addresses and their associated legal owners and physical addresses, then it would be a substantially attractive target for hacking and the privacy and safety of persons in those records would be in profound jeopardy.

Addendum

We thank the FATF for this opportunity to comment and hope that our suggested edits in this Addendum are given a fair consideration in light of the serious human rights and rule of law issues at stake.

Definition of VASP

First, the definition of VASP is described as "expansive" in the final paragraph of the executive summary, in Paragraph 8 of the introduction, and in Paragraph 75 under the subheading "What is a VASP." In all cases, this term should be struck from the guidance. Aside from the general usage of the term "expansive," the following is a list of specific instances where over-expansive language is used to characterize the definition of VASP, as well as suggestions for alternative terms and standards that would be more justiciable:

1. Paragraph 53 where a mere "facilitator" of exchange or transfer services is included
   Suggestion: remove "facilitator" from this list
2. Paragraph 54 where it is proposed that "control does not have to be unilateral and multisignature processes are not exempt"
   Suggestion: remove this sentence and replace with "assumption of independent control over customer assets determines inclusion within the VASP definition"
3. Paragraph 55 where it is proposed that "Service providers who cannot complete transactions without a key held by another party are not disqualified from falling under

[118] Andres Guadamuz, "A Kidnap, a Ransom, and the Limits of Bitcoin as a Criminal Currency," *BREAKERMAG*, January 17, 2019, https://breakermag.com/a-kidnap-a-ransom-and-the-limits-of-bitcoin-as-a-criminal-currency/.
[119] Jason Leopold, et al., "The Fincen Files," *Buzzfeed News*, September 20, 2020, https://www.buzzfeednews.com/article/jasonleopold/fincen-files-financial-scandal-criminal-networks.
[120] Monit Khanna, "8.2 TB Of MobiKwik User Data Allegedly Hacked, Company Denies Breach," *India Times*, March 29, 2021, https://www.indiatimes.com/technology/news/mobikwik-data-breach-hack-credit-card-pan-card-database-dark-web-537273.html.

the definition of a VASP"
Suggestion: replace with "Service providers who cannot complete transactions without a key or keys held by the customer are disqualified from falling under the definition of a VASP"

4. Paragraph 56 where it is proposed that "central part[ies]" merely "creating and launching and asset, setting parameters, holding an administrative 'key' or collecting fees" should be included within the definition of VASP
Suggestion: replace with "central parties holding an administrative 'key' are included if that key affords them independent control over customer assets"
5. Paragraph 57 where VASP would include persons who are "owner/operator(s) of the DApp" and persons who "conduct() business development for a DApp"
Suggestion: replace with "owner/operators of the DApp are included if possession of an administrative 'key' or other credential affords them independent control over customer assets"
6. Paragraph 61 where it is proposed that "control" does not need to be unilateral to be "control"
Suggestion: remove this sentence
7. Paragraph 68 where VASP would include "a party directing the creation and development of the software or platform and launching it for them to provide financial services"
Suggestion: qualify this sentence with "if the party retains independent control over customer assets"
8. Paragraph 72 where inclusion of "governance bod[ies]" for "so-called stablecoins" and persons who "manage the integration of the so-called stablecoin into the telecommunications platform" is proposed.
Suggestion: qualify this sentence with "if the governance body or person integrating the stablecoin into a telecommunications platform retains independent control over customer assets"
9. Paragraph 73 where "changing reserve requirements" for "so-called stablecoins" is included
Suggestion: qualify this sentence with "if changing the reserve requirement or monetary supply involves exercising independent control over customer assets"
10. Box 4 where it is proposed that "Developers are VASPs if they deploy programs whose functions fall under the definition of VASP and they deploy those programs as a business on behalf of customers"
Suggestion: remove this sentence
11. Paragraph 74 where it is proposed that "Only entities that provide very limited functionality falling short of exchange, transfer, safekeeping, administration, control,

and issuance will generally not be a VASP."
Suggestion: remove this sentence

12. Paragraph 75 where "Where the platform facilitates the exchange, transfer, safekeeping or other financial activity involving VAs (as described in limbs (i)-(v) of the VASP definition), then the platform is necessarily a VASP conducting exchange and/or transfer activity as a business on behalf of its customers."
Suggestion: replace "facilitates" with "maintains independent control over VAs while performing"
13. Paragraph 75 where "The FATF takes an expansive view of the definitions of VA and VASP and considers most arrangements currently in operation, even if they self-categorize as P2P platforms, may have at least some party involved at some stage of the product's development and launch that constitutes a VASP. Automating a process that has been designed to provide covered services does not relieve the controlling party of obligations."
Suggestion: remove these sentences
14. Paragraph 76 where it is proposed that "very few VA arrangements will form and operate without a VASP involved at some stage. Where customers can access a financial service, it stands to reason that some party has provided that financial services, even if the act of providing it was temporary or shared among multiple parties"
Suggestion: remove this sentence

Peer-to-peer and privacy prohibitions

1. Paragraph 91(c) which proposes "denying licensing of VASPs if they allow transactions to/form non-obliged entities"
Suggestion: remove subsection (c) in its entirety
2. Paragraph 94 which proposes "A jurisdiction has the discretion to prohibit or limit VA activities or VASPs, and those VA activities carried out by non-obliged entities, based on their assessment of risk and national regulatory context or in order to support other policy goals not addressed in this Guidance (e.g., consumer and investor protection, safety and soundness, or monetary policy).
Suggestion: remove "and those VA activities carried out by non-obliged entities"
3. Paragraph 252 which proposes "VASPs may consider choosing to limit or prohibit transactions with unhosted wallets in this regard"
Suggestion: remove this clause
4. Paragraph 274 which lists "Technological features that increase anonymity" as a red flag indicator.
Suggestion: remove (a) from the list

Recommendation 16

1. Paragraph 91(c): "(e.g., oblige VASPs via the 'travel rule' to accept transactions only from/to other VASPs);"
   Suggestion: remove this parenthetical.
2. Paragraph 156: "The requirements of Recommendation 16 apply to VASPs whenever their transactions, whether in fiat currency or VA, involve: (a) a traditional wire transfer, or (b) a VA transfer between a VASP and another obliged entity (e.g, between two VASPs or between a VASP and another obliged entity, such as a bank or other FI), or (c) a VA transfer between a VASP and an unhosted wallet (i.e. a non-VASP or non-obliged entity). For transactions involving VA transfers, countries should treat all VA transfers as cross-border wire transfers, in accordance with the Interpretative Note to Recommendation 16 (INR. 16), rather than domestic wire transfers, based on the cross-border nature of VA activities and VASP operations. For transfers with unhosted wallets, the requirements of R.16 apply in a specific way, as explained below.
   Suggestion: remove the clause at (c) and the final sentence.
3. Paragraph 179: "In instances in which a VA transfer involves only one obliged entity on either end of the transfer (e.g., when an ordering VASP or other obliged entity sends VAs on behalf of its customer, the originator, to a beneficiary that is not a customer of a beneficiary institution but rather an individual VA user who receives the VA transfer to an unhosted wallet), countries should still ensure that the obliged entity adheres to the requirements of Recommendation 16 with respect to their customer (the originator or the beneficiary, as the case may be)."
   Suggestion: remove this entire paragraph.