Monero Policy Working Group (MPWG)
Date: 20/08/2021

Response to the public consultation on preventing money laundering and terrorist financing – EU rules on public-private partnerships (PPPs)

Submitted by: Monero Policy Working Group
Authors: Dr. F. X. Cabañas; Dr. J. Dubois-Lacoste; Deanna MacDonald; Justin Ehrenhofer; Dr. R. Renwick; Asst. Prof. Dr. A.J. Santos.
Contact: policy@getmonero.org

Introduction

1. The Monero Policy Working Group (MPWG) is a loosely formed quorum of individuals that contribute to the Monero[1] open-source project. Monero is a permissionless, privacy-preserving cryptocurrency network. The goal of MPWG is to work with regulators, policy makers, and the wider financial services sector to ensure a broad understanding of Monero, and other privacy-preserving cryptocurrencies, is communicated. We have specific interest in interacting with entities so they may understand Monero's component technologies, especially in the context of evolving regulatory framework and compliance requirements. We thank you for the opportunity to respond to the European Commission's package of legislative proposals to strengthen the EU's anti-money laundering and countering the financing of terrorism (AML/CFT). We give consent for our contribution to be publicly published in full.

2. We would like to take the opportunity to acknowledge the proposed package. It is far reaching and substantially developed, and we welcome the provisioned ability to respond to the five concurrent public consultations on the matter.

Preventing money laundering and terrorist financing – rules on public-private partnerships

3. We specifically welcome the opportunity to provide input into the Commission's public-private partnership roadmap. However, we feel there are some notable aspects that require careful consideration, especially as they interface with (as noted in the Impact Assessment accompanying the full anti-money laundering package) fundamental rights and freedoms, which are viewed as integral to the European way of life and enshrined by the Council of Europe. We intend to provide further input to the consultation through your

[1] *see* The Monero Project, https://github.com/monero-project and https://getmonero.org.

questionnaire, but will preface our response by providing some high level comment through this avenue.

4. We would like to show our support for aspects of the proposed roadmap. We welcome and commend the intention to request guidance and opinion from the European Data Protection Board (EDPB). It is essential that the intersection between information sharing, regulatory harmonization, the deployment of certain technologies, platforms, shared infrastructures, architectures, and existing data protection legislation have been considered in full - especially as there are considerable risks to both privacy and data protection rights, as well as fundamental rights such as human dignity and autonomy. These may be affected if legislative frames are enacted that alter the balance of investigatory powers[2], surveillance[3], prefigurative politics[4], financial privacy[5], and the presumption of innocence.[6]

5. We welcome clarity, transparency and regulatory oversight of public-private partnerships (PPPs). We acknowledge that PPPs generally seek to alleviate market inefficiencies or complexities inherent in public services,[7] providing a necessary support structure for obliged entities, competent authorities, law enforcement, tax authorities, and financial investigatory units (FIUs). However, private companies and the services they offer are not set up to serve public policy functions, and entrusting private companies to surveil broadly introduces perverse, 'for-profit' incentives. For example, it has been well documented that in the provision of services for PPPs, there is less incentive for the private service provider to invest in enhancing service quality given that any change in the service would require costly contract renegotiation.[8] Specifically, there is a high transaction cost associated with updating privacy policies, data handling and underpinning logic of implemented algorithms. In the context of PPPs for information exchange and surveillance, these services have a direct impact on human rights and people's lives, with the public sector being the final risk-owne. It should also be foregrounded that both negative externalities and indirect costs will be borne by the public.

---

[2] Pol, R. F. (2020). Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. Policy Design and Practice, 3(1), 73-94.

[3] Swire, P. P. (1999). Financial privacy and the theory of high-tech government surveillance. Wash. ULQ, 77, 461.

[4] Husain, S. O., Roep, D., & Franklin, A. (2019). Prefigurative post-politics as strategy: The case of government-led blockchain projects. The Journal of The British Blockchain Association, 1-11.

[5] Ferrari, V. (2020, June). Privacy in Financial Information Networks: Directions for the Development of Legal Privacy-Enhancing Financial Technologies. In International Congress on Blockchain and Applications (pp. 157-160). Springer, Cham.

[6] Tadros, V., & Tierney, S. (2004). The presumption of innocence and the human rights act. The Modern Law Review, 67(3), 402-434.

[7] Sadka, Efraim. "Public-private partnerships—a public economics perspective." CESifo economic studies 53.3 (2007): 466-490.

[8] Välilä, Timo. "How expensive are cost savings? On the economics of public-private partnerships." EIB papers 10.1 (2005): 95-119.

6. The MPWG questions the deployment of certain technologies, algorithms, and surveillance practices without due process and proper care for individuals, data subjects, and finance sector consumers. In the absence of transparency around contracts and due process standards, we fear that certain technologies and practices may become deeply integrated into the public sector without due consideration of their effectiveness, efficacy, proportionality, necessity, or indeed overall legal grounding. It is deeply concerning that the Commission intends to deputize 'for-profit' entities to conduct mass surveillance of EU citizens without first seriously considering the impact on individual liberties, presumption of innocence, and respect for private and family life. We can envision complex litigation cases arising.

7. We recommend the Commission apply a strict regulatory framework incorporating human rights safeguards into the public private partnership procurement policy and contractual liabilities. This should directly inform the metrics used in a human rights impact assessment and monitoring program to be conducted for all PPP contracts undertaken with the Commission, to ensure accountability and compliance. We also recommend that this process be transparent, specifically with respect to the procurement policy and the underpinning contracts with private entities, which should all be made available to the public. This approach for the procurement and continued integration and monitoring of PPPs would - we hope - mitigate a portion of these concerns.

8. The roadmap has indicated a number of high-level themes of investigation that we support. We reiterate our support for due diligence and careful consideration to be given for aspects related (but not limited) to "...antitrust matters and fundamental rights issues, particularly in relation to the rights to protection of personal data, privacy and the presumption of innocence."[9] Further to this, we feel it necessary to highlight specific contextual frames that require consideration by the Commission.

9. The MPWG believes that explicit consideration should be given to the types of technologies that have been, and may be, deployed within PPPs. It is especially important to weigh aspects of proportionality, necessity, risks, and harms against specific implementations employed by the private sector to the public sector (often through profit-seeking contracts). With this in mind, we wish to draw attention to some tools that we feel require consideration, as potential societal harms are wide-ranging, with secondary impacts difficult to quantify without careful consideration.

10. First we consider the use of 'blockchain surveillance', otherwise known as chain analysis, or know your transaction (KYT) techniques, and their application as AML/CTF mitigation measures as provided by one or more PPPs for investigations into crypto assets:

[9] Roadmap - Ares(2021)4733312, Guidance on the rules applicable to the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing, p.2, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13152-Preventing-money-laundering-and-terrorist-financing-EU-rules-on-public-private-partnerships-PPPs-_en

a. It is important to consider that privacy was a primary design consideration in bitcoin. To quote Satoshi Nakamoto: "The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone."[10] We believe that the technical design of public, permissionless blockchains such as bitcoin and monero should make the anonymity of the public keys a necessary precondition for privacy.
b. We believe robust regulation is required to guard against overreliance on 'blockchain surveillance' by supervisory authorities. While the Commission[11] and bodies such as Europol[12] have investigated the efficacy of certain tools and technologies, there are a number of open issues that remain of concern.
    i. There exists a lack of transaction correlation in a significant number of cases using these tools. This becomes apparent when there is a single chain of transactions with no other chains of transactions that merge with it. For example: a single chain of transactions originating from a crypto asset service provider.
    ii. Often algorithms are based on probabilities, and heuristics, which pose considerable risks for innocents, while transactions which occur 'off-ledger' by the trading or theft of private keys might produce a false positive 'red flag' to be associated with an innocent user of cryptocurrency (an illustration of this is provided in Annex A of this submission).
    iii. The MPWG believe those who promote the use of 'blockchain surveillance' as the primarily recommended means of mitigating money laundering and/or terrorist financing risks with crypto assets must also address critical questions regarding the scalability and viability of such methods as the size and utilisation of blockchains increase. 'Blockchain surveillance' can be modelled as the number of ways of choosing K 'dirty' outputs from a set of N total outputs in a blockchain. While the cost of the normal use of a blockchain scales linearly with N, 'blockchain surveillance' scales as the binomial coefficient, N!/(K!*(N-K)!). The question of the scalability of 'blockchain surveillance' as the size of blockchain increases was raised by FinCEN in the United States: "Blockchain analysis can be rendered

[10] Bitcoin whitepaper, Section 10 Privacy, available at: https://bitcoin.org/bitcoin.pdf

[11] Titanium Project (H2020) https://titanium-project.eu/

[12] EUROPOL AND CHAINALYSIS REINFORCE THEIR COOPERATION IN THE FIGHT AGAINST CYBERCRIME, available at: https://www.europol.europa.eu/newsroom/news/europol-and-chainalysis-reinforce-their-cooperation-in-fight-against-cybercrime

less effective by a number of factors, including the scale of a blockchain network".

iv. There are significant adverse effects with the use of 'blockchain surveillance' 'for-profit', especially if these 'for-profit' entities form part of PPPs. In particular, there is a growing tension between 'blockchain surveillance' and current (European Union; California), and proposed (Canada) data protection, privacy, and consumer protection laws. For example, a major 'blockchain surveillance' company is now selling surveillance of customers for marketing purposes, providing a service to profile consumers' economic behaviour. The already existing complexity, uncertainty, and ambiguity associated with risk assessment is further perpetuated and, likely inversely affected, by the profit driven motivations of these entities. Clarification, advisory and oversight is distinctly required in cases of such.

v. Flagging and reporting of 'dangerous' transactions often lacks context and granularity. Broad categorizations used to label and enrich data extracted from blockchain activities, such as 'link to terrorism financing' may be subjective while also being `black boxes' to customers. For example, bitcoin donations to pro-democracy movements in Hong-Kong throughout 2020 would be likely categorized as 'terrorism financing' in China, but not in the EU or US. Similar examples may be made of specific organisations within Member States such as Poland, Hungary, or Romania - to name a few. When the nuances of such categorisations with these tools are left to private companies, there is a high likelihood of inaccurate assessment of risks.

vi. While PPPs are advantageous from a governmental and economic standpoint, we believe chain analysis tools should be fairly and openly distributed to the market - preferably through open-source initiatives, where algorithms are not hidden behind proprietary algorithms and intellectual property law. This economic model has been promoted by the Commission[13] previously, and we urge this to continue.

vii. We note that 'blockchain surveillance' as an AML / CTF tools has been questioned by the FATF[14], and consider blockchain surveillance a prime example of a tool where risks, harms and costs far outweigh the potential benefits resulting in a lack of proportionality or necessity, and where the pursuit of private profit ends up taking precedence over the public good.

---

[13] Graphsense, https://graphsense.info/

[14] Public consultation on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers, footnote 32, available at: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html

11. In the pursuit of robust AML and fraud (both transaction and identity) mitigation, certain tools are being employed within the finance sector that may substantially impact on rights and freedoms of individuals. This has been explicitly noted by the EDPB in their recent opinion on the interplay between PSD2 and GDPR (see Section 2.3).[15] As certain private sector service providers continue to promote data-led device fingerprinting and behavioral-based authentication mechanisms as primary preventative measures, we urge the Commission to consider the impact to individuals, as well as potential for improper use. We feel strict regulation is required to ensure these tools do not take explicit precedence over data protection and privacy rights. We urge the EDPB to be involved in this discussion from the outset.

12. The MPWG is aware that the Commission has explored the possibilities for Distributed Ledger Technology (DLT) based evidential registries to be implemented for robust Know-Your-Customer (KYC) identity verification processes - consulting on the possibility of tying digital identity to online transactions across Europe.[16] While we acknowledge this discussion is part of a wider debate on the nature of digital identity, the proposed amendment of eIDAS, and the proposal for a Digital ID Act - we urge careful consideration if any deployments form part of formal (or informal) PPP agreements. Using distributed ledger based architectures for immutable and verifiable evidential registries poses severe risks to individuals, from technical, organisational perspectives - especially if they are to be governed by for-profit entities who may have considerable incentive to ensure that said registries are used as an infrastructural backbone for behavioural or transactional monitoring. Appropriate regulation *must* be put into place to protect individuals from this outcome, if the deployment of these architectures are to provide net benefit for society.

13. The MPWG believes that data-led AML techniques may increasingly rely on Artificial Intelligence (AI) based technologies, as noted by the European Commission.[17] There is a significant risk of embedded bias in the algorithms deployed by surveillance companies. This may cause harm to underrepresented and marginalised members of society.[18] We draw focus to the large body of work to date documenting algorithmic bias linking disparities relating to race, gender, geo-diversity and socioeconomic status to the performance of

---

[15] Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR, Version 2.0, Adopted on 15 December 2020, Section 2.3, available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid-/public-consultation

[17] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, Recital (37), Recital (80).

[18] Chen, Z., Teoh, E. N., Nazir, A., Karuppiah, E. K., & Lam, K. S. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. Knowledge and Information Systems, 57(2), 245-285.

machine learning models[19] and the correlation between model design choices and the amplification of algorithmic biases for underrepresented subjects[20], including specific risks detailed regarding their use within AML mitigation.[21] We urge the Commission to consider specific regulation protecting the implementation of such within any PPPs.

14. Distinct attention to the use of AI within credit scoring has also noted, including further concerns of bias and discrimination (Recital 37) and the use of AI in transaction monitoring (Recital 80). While competent authorities have been detailed (the European Central Bank), we believe that AI deployed through PPPs may pose substantial risks in the context of both consumer and data protection rights, not to mention imposing on the presumption of innocence. While we do not explicitly doubt the capability of the European Central Bank as a competent supervisory authority in this regard, we believe that formal regulation should be in place to ensure that AI based technologies (and the data that is used to train their algorithms) is not misappropriated by profit-led entities in order to gather insights regarding consumer expenditure, economic behaviour, and economic preferences. We urge the EDPB to be consulted on such.

15. The complexity of risk-based approaches using a combination of publicly-available blockchain data, public and proprietary attribution data, proprietary risk scoring, and individual crypto asset service provider interpretations of potential risk indicators will make enforcement of anti-discrimination laws difficult. When critical financial access tools are abstracted away into multiple AI-driven tools involving several vendors and companies, it can be very difficult to pinpoint the sources of discrimination while marginalized groups are discriminated against in the meantime. Such a task of enforcing non-discrimination laws may be possible, but it would require enormous attention and a dedication to weigh enforcement of these laws over AML enforcement.

16. In summary, we believe the PPP roadmap is a crucial segment of the overarching Action Plan from the Commission, but that a supervisory mechanism should be forthcoming and remains in urgent need. It is not yet clear to us how the legislative framework has become so developed without this critical component. We urge DG-FISMA, EDPB and the Commission itself to consider our opinion and thank the reader for taking the time to consider our response. We welcome any questions that you may have at the email address provided above.

---

[19] Barocas S.Hardt M., Narayanan A. Fairness and Machine Learning. 2019 available at: https://www.fairmlbook.org

[20] See: Buolamwini and Gebru, “Gender shades: Intersectional accuracy disparities in commercial gender classification”: facial-analysis datasets reflect a preponderance of lighter-skinned subjects, with far higher model error rates for dark-skinned women; and Shankar et al., “No classification without representation: Assessing geodiversity issues in open data sets for the developing world.”: models trained on datasets with limited geo-diversity show sharp degradation on data drawn from other locales

[21] Faith, B. A. S. H. J., & Enshaie, A. (2019). Trusting machine learning in anti-money laundering: A risk-based approach. Caspian Learning, Newcastle Upon Tyne, UK, Tech. Rep, available at: http://www.caspian.co.uk/rba/RBA.pdf

Annex A

We acknowledge how the use of blockchain surveillance tools might be manipulated by criminal and / or terrorist elements to facilitate money laundering and / or terrorist financing, while at the same time falsely accusing innocent citizens. We ask the reader to consider the following scenario:

Alice and Bob are EU citizens on holiday in Canada driving their own recreational vehicle. They run into mechanical trouble on a steep mountain road and contact Greg's Heavy Towing for Assistance. Greg's Heavy Towing gets Alice and Bob back on the road, and presents them with the bill of 1421 CAD (~959 EUR).

Greg's Heavy Towing offers a discount of 2% for payments in Cash (CAD), bitcoin or Monero. Greg's Heavy Towing can offer this discount because they can avoid credit card processing fees. Alice and Bob do not have enough CAD in cash, and they want to avoid paying by credit card to earn the 2% discount and avoid the credit card foreign transaction fees. Alice chooses to pay with bitcoin from her personal wallet and obtains an aggregate savings over using her credit card of ~7%. Alice had previously purchased her bitcoin from a crypto asset service provider in the EU which is fully compliant with AML / KYC regulations. Alice and Bob continue with their Canadian road trip, and proceed south to the United States to continue with their holiday, completely unaware of what transpires next.

Later that day, Greg's Heavy Towing receives an unexpected visit from James who represents a criminal organization that is running an extortion racket on various towing companies. James demands the private key to Greg's Heavy Towing's bitcoin wallet containing Alice's payment as protection money. He also threatens Greg the owner with physical harm and the destruction of his business should he not comply with James's demand, contact the authorities, or attempt to move the bitcoin. Greg complies and does not contact the authorities. He also does not interact with the bitcoin wallet.

James proceeds to launder his ill gotten bitcoin by trading the private key he obtained from Greg with the private key that Charlie has. Charlie has obtained his bitcoin from a crypto asset service provider in the United States that is also AML / KYC compliant. This private key trade is attractive to Charlie, because Charlie plans to use the bitcoin towards the purchase of fertilizer and diesel fuel in order to manufacture a bomb for a planned terrorist attack. Charlie does not want the bitcoin traced back to him. James now sells the bitcoin for CAD using a crypto asset service provider in Canada. The crypto asset service provider does not ask any "source of funds" questions of James since they relied on the "clean bill of health" of the bitcoin from the blockchain surveillance company. This in effect replaces KYC with KYT.

The bitcoins were "clean" because they were within the required number of hops from the US crypto asset service provider as per the proprietary algorithm of the blockchain surveillance company. Charlie now proceeds to purchase fertilizer and diesel fuel from different legitimate suppliers with the bitcoin. Again no red flags are raised by the

blockchain surveillance companies since the bitcoins are traced back to the EU crypto asset service provider as "clean". A week later Charlie carries out his terrorist attack. It results in massive casualties in a US Government building. The US authorities trace the fertilizer back to the supplier and a US based blockchain surveillance company traces the bitcoin back to Alice's account at the EU crypto asset service provider. There is no connection found to Charlie. Alice and Bob are arrested in the United States and now face a trial that could potentially result in the death penalty. Their only crime is avoiding 7% in fees charged by various credit card companies. They could also have avoided being falsely accused by using monero as opposed to bitcoin, but the EU crypto asset service provider delisted monero after regulators were lobbied by the blockchain surveillance companies claiming monero was an "anonymity enhanced cryptocurrency", because it broke their proprietary surveillance algorithms.

To understand the scenario there is a critical point. Two criminal transactions: 1) The extortion of the bitcoins from Greg by James and 2) The trade of bitcoin between James and Charlie did not occur on the bitcoin blockchain so they could never be identified by the blockchain surveillance companies no matter how sophisticated their proprietary algorithms.

Many of the elements of this scenario are based on real events:

a) Organized crime involment in the towing industry in Canada https://www.cbc.ca/news/canada/toronto/tow-truck-industry-organized-crime-arrests-1.5583626

b) The Oklahoma bombing and resulting death penalty conviction https://www.theguardian.com/us-news/2015/apr/13/oklahoma-city-bombing-20-years-later-key-questions-remain-unanswered

c) Innocent people facing the death penalty in the US https://deathpenaltyinfo.org/policy-issues/innocence/executed-but-possibly-innocent

In this scenario blockchain surveillance is manipulated in order to facilitate money laundering and terrorist financing. At the same time perfectly innocent citizens are accused of very serious criminal and terrorist acts while the actual criminals and terrorists escape accountability. This occurs simply because of a proprietary algorithm assuming that all the economic activity occurs 'on-ledger'.