10 June, 2019

VIA E-MAIL

Consultation on the Transposition of the Fifth Money Laundering Directive (5MLD)
Sanctions and Illicit Finance Team (2/27)
HM Treasury
1 Horse Guards Road
London, United Kingdom
SW1A 2HQ London
Anti-MoneyLaunderingBranch@hmtreasury.gov.uk

The Electronic Frontier Foundation and Open Rights Group's Response to HM Treasury's Request for Consultation Regarding Transposition of the Fifth Money Laundering Directive

I. Introduction

The Electronic Frontier Foundation (EFF) and Open Rights Group (ORG) welcome the opportunity to respond to HM Treasury's consultation regarding the transposition of the Fifth Money Laundering Directive ("5MLD," EU 2018/843) into national law.

EFF is a non-profit civil liberties law and technology organization. Founded in 1990, EFF champions individual privacy, free expression, and innovation. More than 31,000 individuals worldwide are dues-paying members of EFF. EFF uses public education campaigns, impact litigation, open source technology projects, policy analysis, and grassroots activism to ensure that human rights are protected in the digital age. EFF also allows supporters to make donations through Bitcoin, Ethereum, Litecoin, and Zcash.

EFF's membership includes over 560 members in the United Kingdom and has had the privilege of providing comments for Her Majesty's government and Parliament on previous legislative proposals, including most recently the deliberations by multiple Select Committees prior to the passage of the Investigatory Powers Act,[1] and the consultation held by the Home Office on the

[1] *See* "UK Investigatory Powers Bill" EFF.org, https://www.eff.org/issues/uk-investigatory-powers-bill.

Interception of communications and equipment interference draft codes of practice.[2]

With over 3,000 active supporters, ORG is a UK based digital campaigning organisation working to protect the rights to privacy and free speech. As an online grassroots organisation, ORG has local groups across the UK. Digital technology has transformed the way we live and opened up limitless new ways to communicate, connect, share, and learn across the world. But for all the benefits, technological developments have created new threats to our human rights. ORG raises awareness of these threats and challenges them through public campaigns, media commentary, legal actions, policy interventions, and tech projects.

Our joint areas of expertise in this consultation are twofold: as organizations with decades of understanding of the interaction between technology and human rights, we hope to provide some context on the relationship between the Directive and existing human rights law, especially with regard to free expression and personal privacy.

In addition, our work determining and protecting the growth of free collaboration on the Internet, including the economically significant innovations of free, libre and open source software (FLOSS) development, will, we hope, provide a wider understanding of the effect of regulation within these domains.

II. Executive Summary

As outlined in the Request for Consultation, our submission therefore concentrates on these questions:

- Whether firms “facilitating peer-to-peer exchange services should be required to fulfill AML/CTF obligations on their users, as set out in the regulations. If so, which kinds of peer-to-peer exchange services should be required to do so?” **(Box 2.C: 18)**

- Whether “the publication of open-source software (which includes, but is not limited to, non-custodian wallet software and other types of cryptoasset-related software)” should fall within the scope of the new regulations. HM Treasury asked for “views on whether the publication of open-source software should be subject to CDD requirements. If so, under which circumstances should these activities be subject to these requirements? If so, in what circumstances should the legislation deem software users be deemed a customer, or to be entering into a business relationship with the publisher?” **(Box 2C: 19)**

[2] *See* “Joint Representations by Access, the Center for Democracy & Technology, the Electronic Frontier Foundation, and New America’s Open Technology Institute on ‘Interception of communications and equipment interference: draft codes of practice’” (Mar. 20, 2015), https://www.accessnow.org/cms/assets/uploads/archive/Joint%20GCHQ%20Representation.pdf.

- What approach, if any, should the government take to addressing the risks posed by "privacy coins"? What is the scale and extent of the risks posed by privacy coins? Are they a high-risk factor in all cases? How should CDD obligations apply when a privacy coin is involved?" (**Box 2.C: 25)**

It is our belief that the enforcement steps implied by these new considerations would represent a significant expansion of the regulatory space beyond that determined by 5MLD, and would have an extremely large and unpredictable effect, both on the emerging technology of the blockchain ecosystem, and on the FLOSS software ecosystem at large. Given the relative youth and potential of blockchain innovations, we believe that HM Treasury should tread cautiously. Moreover, any regulation must be sensitive to the fact that FLOSS software underlies a considerable proportion of the modern digital economy — including critical Internet infrastructure, modern financial services, the mobile smartphone ecology, government digital services, and the public and private cyber-security sectors. And, if HM Treasury is intent on broadening its regulatory remit to cover all of these areas, it should separate out this endeavour from 5MLD transposition, into a longer, co-operative initiative with stakeholders across all of these fields.

We must also add that these proposals, if not handled with an understanding of their effect on the privacy and free expression of individuals using or building these tools for legitimate, legal, and human-rights protective purposes, could stand in violation of existing human rights law. This would leave them prone to challenge in the UK courts, the European Court of Human Rights, and, if relevant, the European Court of Justice.

There are substantial benefits to privacy-enhancing technologies such as "privacy coins" and the evolution of peer-to-peer decentralized exchanges; onerous regulation today could stifle these innovations to the detriment of consumers.[3] Furthermore, we urge HM Treasury to recognise that writing and publishing computer code is a protected act of free expression. Thus HM Treasury must consider and incorporate the potential impact on human rights and technological innovation of subjecting FLOSS programmers, and the recipients and users of FLOSS, to regulatory requirements that would interfere with the free flow of knowledge, research, and legitimate expression, as well as insert uncertainty into many unrelated UK industries and public sector institutions that use FLOSS as an essential part of their work.[4]

[3] Mike McConnell, Michael Chertoff, & William Lynn, "Why the Fear Over Ubiquitous Data Encryption Is Overblown," *The Washington Post* (Jul. 28, 2015), https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.

[4] Allison Eck, "Is Code Free Speech?" PBS (Jul. 28, 2018), https://www.pbs.org/wgbh/nova/article/is-code-free-speech/.

III. Responses

HM Treasury Must Value the Privacy Concerns of Consumer Using Peer-to-Peer Exchanges

As the Request for Consultation notes, a cryptoasset is "a cryptographically secured digital representation of value or contractual rights that uses some type of distributed ledger technology and can be transferred, stored or traded electronically."[5] This distributed ledger technology — or blockchain technology — distributes a record of transactions across a network of computers.[6] Its fundamental innovation combines decentralized consensus (ensuring participants settle upon an agreed transaction history) with two important properties: universal access (allowing any entity to publish to this record) and immutability (preventing any individual from tampering with the record). In many cryptoasset applications of blockchain technology, this allows people to securely exchange virtual currencies directly with each other. Because entities can easily audit and verify transactions themselves by consulting the ledger, this removes the need for an intermediary to do so. Bitcoin — the first successful implementation of blockchain technology — was envisioned as a decentralized, or peer-to-peer, electronic payment system that would empower consumers to transact directly with one another without using a third party that might defraud them or otherwise interrupt their transactions.[7]

To perform a transaction on a blockchain (such as transferring cryptocurrency from one user to another), users must acquire the relevant digital currency.[8] For example, to send Bitcoin to another user on the Bitcoin blockchain, a user would first need to acquire Bitcoin. This can be done by "mining" the currency (that is, contributing resources to the decentralized network in exchange for the possibility of obtaining some amount of the currency) or buying the native currency with some other currency (such as pounds sterling). Mining is not always feasible for individuals, so many people obtain digital currencies through centralized exchanges. Blockchains themselves are decentralized, and transactions on blockchains are resistant to censorship. However, centralized exchanges act as choke-points through which users must pass to begin

[5] "Cryptoassets Taskforce: Final Report," HM Treasury at 11 (Oct. 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf.
[6] Dylan Yaga, et al., "Blockchain Technology Overview" at ii, Nat'l Inst. of Standards and Tech., https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.
[7] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" at 1 (2008), https://bitcoin.org/bitcoin.pdf (establishing the concept of Bitcoin as "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.")
[8] Chris Jaikaran, "Blockchain: Background and Policy Issues" at 5-6, Cong. Research Serv. R45116 (2018).

participating in the network.

Many of the examples of mishandling user funds and betraying the trust of customers occur at these centralized choke points, such as cryptoasset exchanges. Centralized exchanges can freeze the funds of customers, block certain customers from the platform, or block specific transactions, with no obligation to provide affected customers with an appeals process. Centralized exchanges can suffer outages, hacks, or losses that prevent customers from accessing their digital currencies.[9] These centralized exchanges are also a target for criminals seeking to steal customer funds, and can themselves be run by unscrupulous individuals who abuse their access to customer funds and data.[10]

By contrast, fully decentralized, peer-to-peer systems often do not need to hold funds for customers — rather, customers can maintain possession of their cryptocurrency, and can exchange their cryptocurrency with others without any intermediary taking possession of the assets. Just one example of such a fully peer-to-peer system is a decentralized cryptoasset exchange, which allows for the exchange of virtual currencies using smart contracts, which enable the automatic execution of more complex transactions without requiring the involvement of intermediaries. For example, requests to sell and purchase virtual currencies can be submitted to a smart contract that matches and completes these exchange transactions. Avoiding centralization means that no intermediary can lose or steal those funds, and no institution holds a honeypot of money that might attract criminals. Furthermore, because such transactions through decentralized systems are not approved by an individual or company, they cannot be easily blocked by a single entity.[11]

These peer-to-peer systems, including decentralized exchanges, are in their earliest stages of development, and many cryptographers and computer scientists are experimenting with other decentralized applications that may have significant public benefit in the long term. Imposing regulatory requirements such as customer due diligence obligations on crypto-asset exchanges could make it difficult for such decentralized systems to operate and innovate. The same centralization that makes it possible to comply with such requirements undermines the important human rights-enhancing and innovative potential of distributed ledger technologies.

[9] *See* Karen Zraick, “Crypto-Exchange Says It Can’t Pay Investors Because Its C.E.O. Died, and He Had the Passwords,” *The New York Times* (Feb. 5, 2019), https://www.nytimes.com/2019/02/05/business/quadriga-cx-gerald-cotten.html .

[10] *See* “Daily Report: Mt. Gox, Having Lost Essentially All Bitcoins, Files for Bankruptcy,” *The New York Times* (Feb. 28, 2014), https://bits.blogs.nytimes.com/2014/02/28/daily-report-mt-gox-having-lost-essentially-all-bitcoins-files-for-bankruptcy/.

[11] Tom Lyons et al., “Blockchain and the GDPR” at 15, EU Blockchain Observatory (Oct. 16, 2018), https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.

The Regulation of the Publication of Open Source Software Would Chill Innovation and Face Challenges under Human Rights Law

Free, libre, and open source software (FLOSS) is software that is distributed in a form that is intended to provide its users with the ability to read and understand completely the nature and function of the software's operations, to modify this software to fit their own needs, and incorporate it into their own creations.[12] Some forms of FLOSS place an additional condition that requires that the further distribution of the code is also licensed in such a way as to preserve these same capabilities for its recipients.[13]

FLOSS has its origins in the shared, peer-reviewed environment of academic learning, but has proven to be a powerful engine of economic growth, innovation, and societal improvement outside academia.[14] By allowing a frictionless method for computer scientists, programmers, and other users of digital technology to share their discoveries, solicit criticism and improvements, and offer others the ability to incorporate these innovations into their own works, FLOSS has increased the productivity of software, and accelerated the dissemination of its benefits. The adoption of FLOSS — both in the form of software produced using this methodology, and the methodology itself — has been widespread, and is now the primary, common form of expression for ideas that are implemented in software.

To give some examples of the breadth of the impact of FLOSS: all the key software that underlies the Internet, from routing of data packets, domain name discovery and provision, the serving of web pages, and the code used to browse those pages, has at least one version written as open source — and generally the most prevalent version. Linux, the primary operating system used on Internet servers, and which underlies the Android mobile operating system, continues to be maintained as a FLOSS project contributed to by thousands of commercial companies, and tens of thousands of individual developers, volunteers, and academics.[15] The UK government, in common with other states, both uses FLOSS and provides its own work for wider use under free or open source licenses. The computer languages used by almost all major commercial sectors to develop their software — including C, C++, Python, Rust, and Java — are open sourced, and rely on an ecology of extensions that are shared and developed in an open source environment.

The entire FLOSS ecosystem relies on the ability of users and developers to be able to download, modify, and share their code without explicit authorisation beyond that granted by the license.

[12] Richard Stallman, "FLOSS and FOSS," GNU.org, https://www.gnu.org/philosophy/floss-and-foss.en.html.

[13] Richard Stallman, "What Is Free Software?" GNU.org, https://www.gnu.org/philosophy/free-sw.html.

[14] *See* David Wheeler, "Why Open Source Software/Free Software?" Appendix 2, https://dwheeler.com/oss_fs_why.html#history.

[15] *See* "2016 Linux Kernel Developer Report", Linux Foundation, https://www.linuxfoundation.org/events/2016/08/linux-kernel-development-2016/

This is not just for purposes of convenience or efficiency. FLOSS code is the group endeavour of large numbers of people, residing in multiple jurisdictions, who are frequently combining and re-writing the code of others to create new features — often anonymously or pseudonymously. A program that may have been started with one level of functionality can quickly be modified to provide for a new context or feature. To give some examples: Linux, now one of the world's most prevalent operating systems, was begun as a student side-project in Finland. PHP, the language that underlay Facebook's services for many years, was originally a tool to allow novice Internet users to quickly build their own "personal home pages", developed at the University of Waterloo by a Danish programmer. Web browsers were originally built to view academic pages (in Switzerland, by a British computer scientist), but have been extended to support complex applications, such as Gmail, and online word processing and spreadsheet software.[16]

Consequently, the functionality of specific open source projects, their authors, and the provenance of its creation and distribution is almost impossible to locate. Code in the open source ecology is almost always built from many other pieces of code: a hundred lines of code used in a cryptocurrency program may have dozens of authors, none of whom wrote it for that purpose because each piece of code will be written as generally as possible. Similarly, code written as part of a cryptocurrency tool may be valuably re-purposed and adapted for other uses.

If the government was to determine that open source software publication should be regulated under money-laundering regulations, it would be unclear how this would be enforced, or how the limits of those falling under the regulation would be determined. Software that could, in theory, provide the ability to enable cryptocurrency transactions, could be modified before release to remove these features. Software that lacked this capability could be quickly adapted to provide it. The core cryptographic algorithms that underlie various blockchain implementations, smart contract construction and execution, and secure communications are publicly known and relative trivial to express and implement. They are published, examined and improved by academics, enthusiasts, and professionals alike. The extent of their application is still being determined, with multiple industries expressing interest in adopting blockchain-based systems into their existing systems of auditing and tracking.

The level of uncertainty this would provide to FLOSS use and provision within the United Kingdom would be considerable; the burden on multiple industries to attempt to guarantee that their software could not be considered part of the infrastructure of a cryptographic money-laundering scheme would be non-negligible. The demands on the Treasury to delineate and arbitrate its reach would be similarly imposing.

The only comparable regulatory initiative may be the United States government's attempt to control the publication and export of public key cryptography in the 1990s. That initiative faced similar challenges. The basic principles of strong cryptography was expressible in a few lines of code; much of the academic research and practical work on the topic was conducted across

[16] "The Birth of the Web," CERN, https://home.cern/science/computing/birth-web.

borders, and required the free expression of such algorithms (often embedded in early open source projects); the difference between theoretical discussion and "dangerous" or unapproved usages was undeterminable at the point of publication. Finally, strong cryptography proved to lie at the heart of an ever-increasing set of commercial and societally beneficial applications, all of which were hampered by regulation intended to limit a smaller set of misuses.

The regulation of public key cryptography was largely abandoned by the same Clinton administration that attempted to introduce them; it had neither limited the spread of strong cryptography, nor managed to limit its ongoing damage to the growing digital economy.[17]

Another parallel was that a key argument against their continued control of strong cryptography was based not on the commercial ramifications, but on human rights principles. Source code is a form of written creative expression, and open source code development is a form of public discourse. The U.S. government belatedly realised that placing restrictions on the publication of certain forms of computer code, would mean regulating publications in general — including printed, physical books which quoted the regulated source code. There is a high burden on states to show that a prior restraint on free expression is legitimate under international human rights law, and successful challenges to the regulation under the United States' First Amendment demonstrated that it was unlikely to survive further judicial review.

Similarly, broad controls on the publication of open source code can expect to face challenges under the Human Rights Act, and if adopted within the European Union, through the European judicial institutions, including the ECJ and European Court of Human Rights.[18]

Undermining "Privacy Coin" Innovation Would Be to the Significant Detriment of Consumer Choice and Privacy

We urge HM Treasury to ensure that regulations do not undermine important innovation in the area of "privacy coins." "Privacy coins" refer to a range of blockchain-based technologies that are using cryptography to enhance individual privacy. "Privacy coins" have the potential to enhance human rights by importing some of the protections that citizens enjoy offline into the

[17] *See* Steven Levy, "Battle of the Clipper Chip," *The New York Times* (June 12, 1994), https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html; *see also* Matt Blaze, "A Key Under the Doormat Isn't Safe. Neither Is an Encryption Backdoor," *The Washington Post* (Dec. 15, 2015), https://www.washingtonpost.com/news/in-theory/wp/2015/12/15/how-the-nsa-tried-to-build-safe-encryption-but-failed/?noredirect=on&utm_term=.0f6bd1210223.

[18] "The Universal Declaration of Human Rights," United Nations General Assembly Resolution 217 A, Article 12 (Dec. 10, 1948), https://www.un.org/en/universal-declaration-human-rights/ ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.").

digital world. Furthermore, any attempt to distinguish between "privacy coins" and non-privacy coins would be problematic.

The increased anonymity and privacy-enhancing features of some cryptocurrencies are part of what makes the technology so potentially important. But many cryptocurrencies are not completely private; most are actually pseudo-anonymous.[19] Transactions are recorded on permanent public ledgers, where users are identified with pseudonymous public keys, with each transaction showing the pseudonymous "account" of the sender and receiver as well as the time and amount of the transaction. Since it potentially broadcasts people's purchases histories, income, and assets to the whole world, this is far less privacy-protective than using cash, or in some circumstances less protective than conventional financial instruments and electronic payment methods. Researchers have already shown a practical ability to identify and track people and organizations from the data in pseudonymous blockchain records, undermining the intuition that cryptocurrencies necessarily provide users with strong privacy or anonymity protections.[20] But there are promising new approaches to developing more private cryptocurrencies, so-called "privacy coins."

Privacy coins seek to increase individual privacy in trading and holding digital assets. While the full impact of privacy coins is likely many years away, future iterations of this innovative technology could help individual consumers engage in modern financial transactions while maintaining their privacy.

Financial transactions can paint an intimate portrait of one's life, exposing religious beliefs, family status, medical history, and many other facets of one's life that might be sensitive and personal. When payees are identified as businesses at a particular physical location (such as a specific café, restaurant, or hotel), financial transaction histories can also reveal a detailed picture of individuals' whereabouts, relationships, and habits. As modern advertising has become more sophisticated, corporations have sought new ways to gather details of our lives. Financial data indicating individual demographics, interests, purchase history, and wealth and income are among the most sought-after types of consumer data.

If they prove technically and economically successful, privacy coins might offer the public the ability to make online purchases with much the same kind of privacy protection that they can achieve offline by paying cash at a bookstore or newsstand — without the prospect that what they purchased will be permanently associated with them, disclosed to other parties, or used as

[19] Merve Can Kus Khalilov & Albert Levi, "A Survey on Anonymity and Privacy in Bitcoin-like Digital Cash Systems" at 8, IEEE (Mar. 26, 2018), https://ieeexplore.ieee.org/document/8325269.

[20] U.S. Sen. Comm. on Banking, Housing, and Urb. Aff., Subcomm. on Nat'l Security and Int'l Trade and Fin., Subcomm. on Econ. Pol'y, 113th Cong. 5-6 (2013) (statement of Jennifer Shasky Calvery, Director, Fin. Crimes Enforcement Network); Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," 57 UCLA Law Rev. 1701 (2010).

the basis for marketing. In the light of Europe's GDPR embodying a principle of "privacy by design and default" and recent decisions by the ECJ upholding the right of individuals to defend themselves against the illegitimate automated processing of their personal data, privacy coins better reflect the degree of confidentiality provided by existing financial services, as well as the expectations of consumers, legislators, and the courts.

We are concerned that onerous regulations adopted today to address the UK government's concerns would directly impact everyday UK citizens who have committed no crimes. Short-sighted regulations could dissuade British citizens from holding or using privacy coins, or might push privacy-enhancing innovation out of the UK's blockchain community. This would ultimately rob British citizens of opportunities to access potentially significant and protective technologies.

Furthermore, a legal distinction between "privacy coins" and non-privacy coins is difficult to draw with precision at this stage. All cryptocurrencies use cryptographic means to authenticate transactions without linking them to an offline identity. Current experiments and proposals in the field of privacy-enhancing cryptocurrencies offer a broad range of different privacy properties under different circumstances and threat models, including treating different sorts of payment-related data as private or public by design (e.g., persistent identities of transaction senders or recipients, temporary pseudonyms, the existence of a transaction, the value of a transaction, the source of funds for the transaction, the relationship or non-relationship among a number of separate transactions, the current assets held by individual participants in the system, other metadata associated with a transaction, as well as whether or not transaction participants can choose to voluntarily reveal additional details after the fact). Further research is also needed to confirm to what extent privacy protections apparently provided by a particular system are actually realised in practice and can resist future technical efforts to defeat them.

A broad attempt to define privacy coins with an eye to restricting their development and use in the UK would be unreasonable and premature. Instead, we urge the UK government to consider privacy coins as a powerful new tool for everyday citizens to protect their financial privacy in the digital age. As the UK government considers how to handle privacy coins in the future, we urge regulators to consider the benefits to consumers of this technology. Regulations that could fundamentally change the privacy-enhancing benefits of these new privacy coins could ultimately prove significantly detrimental to consumer rights.

IV. Conclusion: Prioritising Privacy, Free Expression and Innovation in the Expansion of AML/CTF Regulations

We appreciate the opportunity to submit comments expressing the significant human rights impact of the proposed regulations. As HM Treasury continues to chart a course to combat the abuse of financial systems for crime and terrorism, we urge the Treasury to ensure protection of core human rights such as individual privacy and freedom of expression. We also hope the

Treasury will recognise the broader consequences of any attempt to control the publication of open source software, and instead seek to target the active misuse of technology, rather than limit the exploration, academic review, and innovation in these emerging technologies.

We recognise that in seeking to clarify the implementation of 5MLD in a rapidly-evolving digital environment, the UK government is not necessarily “gold-plating” the mandate of the Directive. But the risk remains that in widening the scope of the 5MLD to include privacy coins, open source software publication, and peer-to-peer exchanges, any transposed legislation will, in fact, result in an even worse scenario. Rather than simply going beyond the Directive in its approach to money-laundering, the UK implementation, if broadened in this way, will cause profound economic disruption in fields entirely unrelated to lawful and unlawful financial transactions. It will also undermine the UK’s premier position as innovators in modern financial services, and risk the entire project of fighting modern money laundering by making the legislation susceptible to challenges under domestic and international human rights laws and principles.

Sincerely,

Danny O’Brien
Electronic Frontier Foundation
+1 415 436-9333
danny@eff.org

Jim Killock and Alan Cox
Open Rights Group
0207 096 1079
jim.killock@openrightsgroup.org