Comments to Her Majesty's Treasury on Transposition of the Fifth Money Laundering Directive

Peter Van Valkenburgh
June 7, 2019

Introduction

Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing digital currency 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 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 the opportunity to comment on HM Treasury's public consultation regarding transposition of the Fifth Money Laundering Directive.

The consultation describes two options for UK financial surveillance policy towards cryptoasset stakeholders: (1) transposing the minimal harmonizing requirements found in the European Union's Fifth Money Laundering Directive (5MLD), or (2) transposing the minimum requirements alongside additional provisions.[1] Coin Center strongly urges HM Treasury to limit itself to the first alternative: merely transposing the minimal requirements.

To the extent HM Treasury finds it absolutely necessary to go beyond 5MLD or seeks alternative models for developing financial surveillance policies towards these technologies, we suggest seeking parity with the current approach taken in the United States. The first portion of this comment will briefly summarize the recent interpretive guidance released by the relevant US regulator, the Treasury Department's Financial Crimes Enforcement Network (FinCEN), such that the UK can develop a harmonious approach. In brief, FinCEN has developed a reasonable interpretation of the underlying US statutory law, the Bank Secrecy Act (BSA), that would include within scope any intermediaries who both accept and transmit fiat and/or cryptoassets from one person to another or from one location to another. In other words, the scope is limited to persons who have, at least momentarily, independent control over the fiat and/or cryptoassets of their customers in order to transmit those valuables on their behalf.

[1] HM Treasury, "Transposition of the Fifth Money Laundering Directive," Consultation (Apr. 2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf.

Coin Center strongly urges HM Treasury to avoid developing any provisions additional to the 5MLD that would expand the scope of regulated parties beyond those regulated under the BSA according to FinCEN's interpretive guidance.

Thus far, HM Treasury—alongside the Financial Conduct Authority (FCA)—has developed a reasonable, proportionate, and flexible regulatory regime for cryptoassets that has made the UK a welcoming home for blockchain innovation while simultaneously addressing key policy issues such as consumer protection, prudential regulation, and crime prevention. Indeed, the UK's approach has been cause for envy from innovators in the US and other nations.[2]

Expanding the scope of regulation beyond 5MLD and the current approach in the US could rapidly reverse this pro-innovation stance and—in the longer run—may leave the UK substantially behind the curve in financial technologies. A bespoke approach that goes beyond 5MLD and the US BSA would fragment international standards, burden regulated parties without concomitant benefit to law enforcement, and endanger the civil and political rights of UK citizens.

Coin Center is particularly alarmed by two potential scope expansions discussed in the consultation: the inclusion of "peer-to-peer exchange service providers" and the inclusion of persons engaged in the "publication of open-source software."[3] Bringing software publishers and other non-custodial entities (who may nonetheless facilitate peer-to-peer exchange) within the scope of regulation would be severe overreach. It would, in effect, necessitate a gross curtailment of free expression within the UK and impose an arbitrary electronic surveillance regime unbounded by law and due process.

As echoed by the Delegated Powers Committee, any such overreach in the arena of money laundering regulation may violate the rule of law if it is attempted via secondary legislation alone rather than through primary legislation.[4] Moreover, regulatory and discretionary overreach that limits the essential speech and privacy rights of UK citizens without a sufficiently clear statement of law to temper the discretion of authorities would likely be in violation of the European Convention on Human Rights.[5]

FinCEN's Interpretive Guidance and Independent Control

On May 9, 2019, FinCEN issued new guidance (the Guidance) on how the BSA applies to cryptocurrencies and the businesses and individuals who use them.[6] The Guidance focuses on

---

[2] *See generally*, Jeff Lynn, "Why Britain is beating the U.S. at financial innovation," *TechCrunch* (May 2016) http://techcrunch.com/2016/05/13/why-britain-is-beating-the-us-at-financial-innovation/.
[3] HM Treasury, "Transposition of the Fifth Money Laundering Directive," Consultation (Apr. 2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf.
[4] https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/38/38.pdf
[5] *See*: Council of Europe, "European Convention on Human Rights," Articles 8 and 10, *European Court of Human Rights*, https://www.echr.coe.int/Documents/Convention_ENG.pdf.
[6] U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," Guidance

answering the same question of scope that HM Treasury raises in its consultation. The Guidance does not depart substantially from existing policies first developed by FinCEN in 2013, but it does describe several "common business models" for cryptoassets in detail and explain why or why not each business model would be within the scope of the BSA.

The following aspects of the Guidance are particularly relevant to the consultation's questions on scope:

1. FinCEN does not discriminate between fiat-to-cryptoasset and cryptoasset-to-cryptoasset exchange. Anyone accepting and transmitting "currency" (fiat) and/or "currency substitutes" (a broad category that includes cryptoassets) is likely to be within scope.[7] Incorporating what the consultation calls crypto-to-crypto exchange service providers into scope would merely bring parity with policies the US has had in place since 2013.
2. FinCEN interprets the BSA such that only persons who have "independent control" over another person's cryptoassets can, in fact, accept and transmit value. Therefore persons who may facilitate exchange or transmission, but who do not have independent control (*e.g.*, open source software developers, multiple-signature service providers, and decentralized exchange facilitators), are not within scope.[8] Bringing these entities within scope is highly problematic for reasons discussed below.
3. Privacy-preserving cryptocurrencies, what the consultation refers to as "privacy coins," are discussed in the Guidance, and FinCEN finds that the software developers who work on these tools and projects are out of scope but that custodial privacy-enhancing services are within scope.[9]

We will describe points two and three in a bit more depth because they provide a sensible and articulable legal principle for who should and should not be within the scope of regulations. While FinCEN's interpretive guidance does not, of course, have any precedential or even persuasive legal authority over proceedings in the UK, it is nonetheless an approach that has proven itself over the last six years to be reasonably permissive of innovation while remaining sufficiently comprehensive to provide law enforcement with the tools and information necessary to fight crime. Notably, the US Department of Treasury has clear and sufficient statutory authority to further expand the scope of the BSA through rulemaking, but it has refrained from doing so, choosing instead to simply interpret the existing rules with respect to cryptoassets in the Guidance and associated administrative rulings.[10]

FIN-2019-G001 (May. 9, 2019) https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf.

[7] *Id*.

[8] *Id*.

[9] *Id*.

[10] U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Virtual Currency Mining Operations," Guidance, FIN-2014-R001 (Jan. 2014) https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R001.pdf; U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Certain

Software Wallets, Multi-Signature Service Providers, Decentralized Exchange, and Independent Control

Section 4.2.1 of the Guidance states that software wallet providers (*i.e.*, "non-custodial" or "unhosted" wallet providers) are not regulated as money transmitters and are therefore not within the scope of the BSA. Section 4.2.2 states that so-called multiple-signature wallet providers without the ability to unilaterally transact with customer funds are also not regulated as money transmitters. All of these parties generally engage in what the consultation describes as the "publication of open source software." Indeed, multiple-signature wallet providers often publish wallet software and, additionally, provide a valuable security service to wallet users by co-signing transactions out of the wallet, subject to fraud checks or other policies designed to prevent theft.[11]

Describing these non-custodial multiple-signature wallet providers, the Guidance states: "the person participating in the transaction to provide additional validation at the request of the owner does not have total independent control over the value."[12] If a person develops and publishes the multiple-signature wallet software and limits herself to providing this "additional validation" then she is not within the scope of BSA regulation. As the Guidance states:

> If the multiple-signature wallet provider restricts its role to creating un-hosted wallets that require adding a second authorization key to the wallet owner's private key in order to validate and complete transactions, the provider is not a money transmitter because it does not accept and transmit value.[13]

Section 5.1 states that decentralized exchanges (DEXs, *i.e.*, non-custodial exchanges) are not regulated as money transmitters for similar reasons:

> [I]f a [Convertible Virtual Currency (CVC)] trading platform only provides a forum where buyers and sellers of CVC post their bids and offers (with or without automatic matching of counterparties), and the parties themselves settle any matched transactions through an outside venue (either through individual wallets or other wallets not hosted by the trading platform), the trading platform does not qualify as a money transmitter under FinCEN regulations.[14]

In both these examples, FinCEN has articulated a clear underlying legal standard for the scope of BSA regulation. Persons who have actual and independent control over the cryptoassets of

---

Business Models Involving Convertible Virtual Currencies," Guidance, FIN-2019-G001 (May. 9, 2019) https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf.

[11] Ben Davenport, "What is Multi-Sig, and What Can It Do?," *Coin Center* (Jan. 1, 2015) https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do.

[12] U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," Guidance, FIN-2019-G001 (May. 9, 2019) https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf.

[13] *Id.*

[14] *Id.*

others will be regulated; however, merely providing someone with software, services, or tools that enable them to move or control their own cryptoassets is out of scope.

Privacy-Preserving Cryptocurrencies, Software, and Services

The consultation asks, "What approach, if any, should the government take to addressing the risks posed by 'privacy coins'?" FinCEN's Guidance offers an interpretation of how these new tools fit within existing US law. Section 4.5.1 states that mere developers of privacy-preserving cryptocurrencies or protocols are not within scope. This section draws a critical distinction between those who provide **services** that can anonymize cryptocurrency payments and others who only write or publish **software**. In both cases the Guidance considers cryptoasset tumblers and mixers as well as privacy-preserving cryptocurrency networks themselves. For example, one can think of a mixer *service* provider (which receives coins from users, shuffles all the coins, and sends them back to its users) on the one hand, or one can think of mixer *software* (which is merely a protocol that allows participants in a mix to move money to and from each other without any service provider in the middle *e.g.*, TumbleBit protocol) on the other. Similarly, one can think of privacy-preserving cryptocurrency network *software* (*e.g.*, Monero or Zcash) on the one hand, and on the other a centralized *service* (*e.g.*, Liberty Reserve or e-Gold) that keeps no records of user transfers.

This distinction is significant because, according to the Guidance, *service* providers are money transmitters and therefore within scope while *software* providers are not:

> An anonymizing software provider is not a money transmitter. FinCEN regulations exempt from the definition of money transmitter those persons providing 'the delivery, communication, or network access services used by a money transmitter to support money transmission services.' This is because suppliers of tools (communications, hardware, or software) that may be utilized in money transmission, like anonymizing software, are engaged in trade and not money transmission.[15]

Section 4.5.3 states that custodial exchanges (which are, of course, within scope) are not *per se* prohibited from using privacy-preserving cryptocurrencies as part and parcel of their BSA compliance obligations, but will need to comply with the same BSA regulations applicable to less-private cryptoasset transactions. This means that custodial exchanges need to know their customers but they do not and should not have a requirement to know the people their customers ultimately pay using privacy protecting cryptocurrency withdrawn from their account. More succinctly stated, custodial exchanges do not need to know the customers of their customers if the exchange is not the intermediary in those transactions. This mirrors existing money laundering policy in the world of traditional finance: a bank needs to know its account holders and may need to know the ultimate recipients of wire transfers from those

[15] U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," Guidance, FIN-2019-G001 (May. 9, 2019) https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf.

account holders to other banks, but banks are not obligated to know the name and address of people that their account holders pay using cash withdrawn from their accounts, such a requirement would be plainly unworkable with physical cash and it would also be a substantial intrusion upon persons' legitimate privacy interests. Privacy-protecting cryptocurrency transactions are effectively like cash transactions and should be regulated similarly.

With respect to transfers between regulated intermediaries and the need to send customer data, it is worth noting that many of the more popular privacy-preserving cryptocurrencies allow for an encrypted messaging field that can be used for compliance with the US "travel rule" or the EU equivalent, the "wire transfer rule."[16]

As with cash, these tools can and will be used for illicit purposes; they are also, however, essential tools for maintaining personal privacy, and checking the power of oppressive regimes or unscrupulous data monopolies. Prohibiting their use, even if there is some evidence of crime facilitation, is simply not compatible with liberal values and the preservation of an open society.[17]

The FinCEN Guidance and International Standards

FinCEN's commonsense clarifications of scope stem directly from a sensible interpretation of underlying US statutory law. The UK has entirely different underlying law; however, the approach taken by FinCEN creates a reasonable and articulable legal principle for who may and may not be deputized as an agent of state surveillance, and, as such, is a valuable model. FinCEN's standard is very clear: only persons who have independent control over customers' cryptoassets are within the scope of regulation.

As we will explain in the next section, any attempt to broaden the scope of regulated parties to include persons who do not have independent control of others' cryptoassets (*e.g.*, developers and facilitators of cryptoasset software, peer-to-peer exchange, or network infrastructure) would severely curtail the speech and privacy rights of UK citizens as well as fail to establish a reasonable and articulable legal principle for who may and may not be deputized as an agent of state surveillance. We therefore recommend that the FinCEN guidance serve as a limiting model for any additional provisions the UK chooses to adopt beyond 5MLD.

[16] "Zcash transactions also have a memo field that can be used to send additional data about the transaction viewable only to the recipient. This memo could carry data between financial institutions wherever they are required by law to send that data along (e.g. the "travel rule" requirement in the Bank Secrecy Act)." *See*: Zooko Wilcox and Peter Van Valkenburgh, "What is Zcash?" *Coin Center* (Dec. 8, 2016) https://coincenter.org/entry/what-is-zcash.

[17] Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash.

Including Software Developers Within the Scope of Regulation Would Severely Curtail the Speech and Privacy Rights of UK Citizens

Coin Center has recently published a comprehensive report describing the fundamental technologies behind cryptoassets (in particular, privacy-preserving cryptoassets, which we call "electronic cash") and decentralized exchange software.[18] The report explains why regulating the developers of these technologies in the US as BSA obligated entities would violate both the First and Fourth Amendments of the US Constitution. While the UK does not have analogous, written First and Fourth Amendment rights, it is a nation with a profound and ancient respect for the rule of law as well as a bound signatory of the European Convention on Human Rights and the International Covenant on Civil and Political Rights.[19] As such, several of the underlying principles that would forbid US regulators from deputizing open-source developers or other non-custodial entities as compulsory participants in a state surveillance regime similarly limit regulators in the UK. In the following, we have condensed and amended portions of our report for the benefit of HM Treasury's consultation.

At heart, developing electronic cash or decentralized exchange software is an academic engineering challenge like any other. It is an exercise in free thought and free speech. As with any creative endeavor, there's prior work from which to draw inspiration: decades of computer science research,[20] cryptographic literature,[21] and existing cryptocurrency software, which for all major networks is open-source and available for study without payment or licensing.[22] There's creative and innovative work to be done: forging new mathematical proofs, translating old ideas into new languages, and combining past work into novel and useful arrangements. As with any scientific inquiry, this process is ongoing and never-ending, and literally thousands of people around the world are actively contributing to the body of research.[23] Periodically there are published results, both academic papers written in prose that describe new software tools as well as the software itself, written in a range of common coding languages.

---

[18] Peter Van Valkenburg, "Electronic Cash, Decentralized Exchange, and the Constitution," *Coin Center* (Mar. 2019) https://coincenter.org/entry/e-cash-dex-constitution.
[19] Council of Europe, "Chart of signatures and ratifications of Treaty 005," *Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS No.005 (Sep. 1953) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=EAEWQz4R; United Nations, "Status of Treaties," *International Covenant on Civil and Political Rights* (Dec. 1966) https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND.
[20] Arvind Narayanan and Jeremy Clark, "Bitcoin's Academic Pedigree," *Communications of the Association for Computing Machinery*, Vol. 60, No. 12 (Dec. 2017): pgs. 36-45, https://users.encs.concordia.ca/~clark/papers/2017_cacm.pdf.
[21] *See*, *e.g.*: Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *ACM Transactions of Programming Languages and Systems*, Vol. 4, No. 3 (Jul. 1982): pgs. 382-401, https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf.
[22] *See*, *e.g.*: The Bitcoin Core GitHub repository (https://github.com/bitcoin/bitcoin).
[23] Bitcoin and Ethereum core client software alone have over 1000 individual contributors and that number does not include the countless developers working on compatible software for wallets, miners, smart contracts, or countless developers working on other cryptocurrencies. Nor does that number include the several academic authors who have published peer-reviewed research on these systems.

Those published results, on their own, do not create electronic cash or decentralized exchange. Instead, the published software explains—in exacting detail—how one would make an electronic cash transaction or a decentralized exchange. Software is not self-executing; it's a set of instructions, like a recipe for a meal or a musical score for a performance. Once published, it's up to people around the world to follow those instructions.[24] Software makes this a bit easier than performing a Beethoven sonata or baking a soufflé, because the instructions are so complete that they require little skill or improvisation and because their users can exploit a machine that can read the instructions—a computer—to do most of the work. But the users are essential nonetheless: they must run the software on their internet-connected computers, and it's only once those computers start working together as a network[25] that some usable functionality, such as electronic cash or decentralized exchange, becomes possible.

The primary effect of these advances in technology are cryptocurrency networks that protect the privacy of their users. Developers and advocates genuinely believe that such tools are necessary to protect human dignity and autonomy, and argue that they are of profound political and societal importance in a world where transactions are increasingly surveilled and controlled by a handful of private financial intermediaries and powerful governments.[26] A secondary effect of these advances is significantly less visibility into cryptocurrency transactions for regulators and law enforcement. Thanks to electronic cash transactions, data that would otherwise be public on a blockchain may now be private to the transacting parties, and, thanks to decentralized exchange, many users seeking to exchange their cryptocurrencies for other cryptocurrencies may do so directly with each other rather than through a regulated third party, which could collect customer information.

Faced with this reduction in surveillable information, governments may seek to extend anti-money-laundering surveillance obligations to electronic cash or decentralized exchange software developers or users. Such an extension, however, would be in violation of Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[27] and Article 8 of the European Convention on Human Rights (ECHR) (collectively, international privacy rights).[28] Additionally, the resulting arbitrary intrusions upon privacy would violate foundational rule of law principles as originally articulated in the English common law in *Entick v. Carrington*.[29] Similarly,

---

[24] You can try it for yourself by following the directions to install Bitcoin here: https://bitcoin.org/en/getting-started.
[25] You can see a visualization of the global nodes on the Bitcoin network at Bitnodes: https://bitnodes.earn.com/nodes/network-map/?ipv6_bits=56.
[26] Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash.
[27] 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.
[28] 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
[29] *Entick v. Carrington* (1765) 19 St Tr 1030.

governments may seek to ban or permission the distribution electronic cash software that does not collect user information, or they may compel developers to surreptitiously introduce surveillance-friendly vulnerabilities or backdoors into their software; this would be in violation of Article 19 of the ICCPR and Article 10 of the ECHR (collectively, international expression rights). Each of these arguments, privacy and expression, will be discussed in turn.

Privacy Rights

Both the ICCPR and the ECHR prohibit intrusions upon the privacy of persons unless those intrusions are made in accordance with law. As the European Court of Human Rights found in *Malone v. the United Kingdom*, "the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention."[30] As the court found, "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence."[31]

Any attempt to treat open-source software developers as within scope would, in effect, deputize those software developers who choose to comply as agents of HM Treasury tasked with indiscriminately collecting information on the users of their software. Those developers who fail to comply would be, it stands to reason, banned from distributing their software in the UK. As such, persons in the UK who choose to engage in cryptoasset transactions of any kind would be forced to use software that collects information about their activities by government decree irrespective of their particular circumstances and without their forming any business-customer relationship with a financial institution or other entity.

As a result, everyone who chooses to use cryptoassets would, by default, be surveilled. The resulting mass collection of otherwise private information irrespective of any particular suspicion, warrant, or legal process is not compatible with the rule of law as there are no "sufficiently clear terms" describing "the circumstances in which and the conditions on which public authorities are empowered" to intrude upon the privacy of UK citizens. As the court in *Entick v. Carrington* famously held, "If it is law, it will be found in our books. If it is not to be found there, it is not law… By the laws of England, every invasion of private property, be it ever so minute, is a trespass… If no excuse can be found or produced, the silence of the books is an authority against the defendant, and the plaintiff must have judgment."[32]

Even if HM Treasury was to carefully spell out the breadth of such a surveillance regime explicitly in law (*e.g.*, *users of cryptoasset software will be surveilled in all situations irrespective of any particular suspicion of wrongdoing, due process, or warrant*) the policy would remain violative

[30] Malone (James) v United Kingdom, Judgment (Merits), App No 8691/79 (A/82), [1984] ECHR 10, (1984) 7 EHRR 14, IHRL 47 (ECHR 1984), 2nd August 1984, European Court of Human Rights [ECHR].
[31] *Id*.
[32] *Entick v. Carrington* (1765) 19 St Tr 1030.

of international privacy rights. As the UN Committee on Human Rightshas 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*…
>
> 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].[33]

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. Such an approach is not and cannot be compatible with case-by-case decision making.

As mentioned earlier, similar prohibitions on warrantless search, warrants of general application, and bulk surveillance regimes exist in the US constitutional tradition. We will not rehearse those arguments here because of their specificity with regard to US rather than UK law. However, these arguments are nonetheless illustrative of how bulk collection regimes, bans on cash transactions, and similar bans on electronic cash technologies are incompatible with liberal values and an open society. We urge HM Treasury to review our previous reports on electronic cash and decentralized exchange if it wishes to learn more.[34]

Speech Rights

As discussed earlier, 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

---

[33] 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.
[34] Peter Van Valkenburg, "Electronic Cash, Decentralized Exchange, and the Constitution," *Coin Center* (Mar. 2019) https://coincenter.org/entry/e-cash-dex-constitution; Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash.

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.

Indeed, the "unfettered interchange of ideas"[35] 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*.[36] 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.[37]

---

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

[36] 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.

[37] *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/.

Moreover, open-source computer code underlies systems we rely upon daily to organize our society—from email clients to traffic lights, police surveillance cameras to social networking websites and—more recently—private decentralized money and exchange. Everything we do (and cannot do) on those platforms and with those tools is mediated by software and ideas expressed in code. Anyone can learn to read the languages in which this code is written in order to elevate and formulate their view of debates surrounding these technologies, and anyone who has learned those languages can invent and suggest new and different ideas, including alternatives to the systems of today. Developers may learn these skills because they think they can build better, safer tools for organizing society, enabling individual freedom, or limiting the freedom of those who would do others harm.

Say what one will about the deservedly mocked mantra of Silicon Valley, "make the world a better place," but software does make the world.[38] Source code and the creative and scientific expression it contains now represents a substantial quantity of the world's "ideas for the bringing about of political and social changes desired by the people."[39] Many remain surprised and even alarmed that a new language—many new languages in fact—are actively being used to fundamentally reshape the landscape of human interaction. But to deny this fact is to deny everything that has changed in our lives since the advent of digital computing. Similarly, to deny statements made in coding languages like C++[40] or Rust[41] the same constitutional protections we would grant statements made in English would make no more sense than to deny novels protection when they are written in French, symphonies protection because they are written in musical notation, or scientific papers protection because they tend to be filled with arcane graphs and formulae.

With certainty we can say that thousands of persons independently work to publish open-source cryptoasset software. 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 offering the FCA or HM Treasury discretion to decide which versions of this software can and cannot be published and shared among UK citizens 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

---

[38] *See, e.g.*: "Silicon Valley, TechCrunch Disrupt Parody," *goodlaugh182 YouTube Channel* (May 25, 2014) https://www.youtube.com/watch?v=J-GVd_HLlps.
[39] *Roth v. United States.*
[40] *See, generally:* Bjarne Stroustrup, "The Essence of C++," *The University of Edinburgh YouTube Channe*l (May 4, 2014) https://www.youtube.com/watch?v=86xWVb4XIyE.
[41] *See, generall*y: Steve Klabnik and Carol Nichols, *The Rust Programming Language*, San Francisco, CA: No Starch Press (2018) *available at* https://doc.rust-lang.org/book/ch00-00-introduction.html.

protocols; whose responsibility is it 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 UK 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. The majority of these publishers are not even located in the UK and would not be subject to the law.

Even assuming that some versions of cryptoasset software do end up having backdoors because of an order from a UK regulator, how can the regulator ensure that the several other versions of cryptoasset software lacking backdoors are not published and shared amongst UK 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 the UK. 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.[42] Would the UK 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 and Article 10 of the ECHR. Both conventions hold that persons should have "the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."[43] Both conventions find that the exercise of these rights carries "special duties and responsibilities" that justify a limited range of restrictions on speech.[44] 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."[45] 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 UK citizens to regulate their own conduct.

Nor would a blanket ban on cryptoasset software publication withstand constitutional scrutiny. Specifically in the context of software and the internet, UN General Comment No. 34 to Article

[42] Adam Back, "Munitions T-shirt," accessed June 6, 2019, http://www.cypherspace.org/adam/uk-shirt.html.
[43] *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.
[44] *Id*.
[45] *Id*.

19 of the ICCPR finds that "generic bans on the operation of certain sites and systems" are not compatible with the ICCPR.[46]

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."[47] 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.

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."[48] As described in the first half of this comment letter, regulators such as FinCEN have developed policies which have, over the last six years, reasonably addressed the threats of money laundering without stifling the free exchange of ideas and the 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.

Electronic cash and decentralized exchange software includes a broad class of published research and innovations with far-reaching potential to alter the way we organize society. Its developers and advocates genuinely believe that these scientific and engineering advances will, on net, improve the human condition and better guarantee human dignity and individual autonomy than alternative centralized and surveillance-accommodating tools for payments and exchange.[49]

A primary motivation behind the development of this technology is the global decline of cash transactions (which are inherently private and lacking in intermediaries).[50] 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.[51] If cash disappears, advocates claim, only electronic cash and

---

[46] 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.
[47] *Id*.
[48] *Id*.
[49] Jerry Brito, "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center* (Feb. 2019) https://coincenter.org/entry/the-case-for-electronic-cash.
[50] *Ibid.*
[51] *Id.*

decentralized exchange technologies can serve as a safety valve against imminent payments-technology-enforced totalitarianism.[52]

One does not need to personally subscribe to these views in order to grasp the gravity of the constitutional law at hand. It is sufficient to believe that electronic cash and decentralized exchange 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 and Article 10 of the ECHR.

Proposed Limitations Upon Speech and Privacy Cannot be Made Through Secondary Legislation

The UK's exit from the European Union has necessitated the creation of new primary legislation, the Sanctions and Money Laundering act of 2018, to establish HM Treasury's statutory authority with regard to money laundering regulation.[53] The relevant portion of that legislation reads as follows:

> (49) An appropriate Minister may by regulations make provision for one or more of the following purposes—
>
> (a) enabling or facilitating the detection or investigation of money laundering, or preventing money laundering;
>
> (b) enabling or facilitating the detection or investigation of terrorist financing, or preventing terrorist financing;
>
> (c) the implementation of Standards published by the Financial Action Task Force from time to time relating to combating threats to the integrity of the international financial system.

Thus the appropriate minister is permitted to develop a range of money laundering policies in the UK subject only to up-or-down affirmation from parliament. The Legislative and Regulatory Reform Act of 2006 establishes limits as to what policies can be established through mere regulation (*i.e.*, secondary legislation) and what policies would require primary legislation. It reads in part as follows:

> (1) A Minister may not make provision under section 1(1) or 2(1), other than provision which merely restates an enactment, unless he considers that the conditions in subsection (2), where relevant, are satisfied in relation to that provision.
>
> (2) Those conditions are that …

[52] *Id.*

[53] Previous authority was derived from the European Communities Act of 1972. New legislation is the Sanctions and Anti-Money Laundering Act of 2018, *available at* http://www.legislation.gov.uk/ukpga/2018/13/pdfs/ukpga_20180013_en.pdf/

(e) the provision does not prevent any person from continuing to exercise any right or freedom which that person might reasonably expect to continue to exercise;
(f) the provision is not of constitutional significance.[54]

Similarly, Section 7 prohibits policy changes in secondary legislation that would

(a) authorise any forcible entry, search or seizure; or
(b) compel the giving of evidence.

As discussed in the previous sections, an expansion of scope to include open source software developers or persons facilitating decentralized exchange would:

- Substantially impact the privacy and speech rights and freedoms that persons in the UK expect to exercise.
- Be of grave of constitutional significance due to blanket surveillance's incompatibility with the rule of law and the foundations of English common law, and
- Authorize searches of every person in the UK utilizing these technologies and compel the production of evidence that may be used against them.

Thus, Coin Center believes that HM Treasury cannot adhere in good faith to the strictures of the Legislative and Regulatory Reform Act if it chooses to implement policies that would subject open-source software developers or persons facilitating decentralized exchange to money laundering regulations.

The Delegated Powers Committee has already voiced its concerns over the breadth of powers granted to ministers under the Sanctions and Money Laundering Act:

> The wording [of the relevant portion of the act], in setting out the scope of the powers, is very broad. It refers to making provision for the purposes of the prevention, detection and investigation of money laundering and terrorist financing. Each of 'prevention', 'detection' and 'investigation' are liable to cover a very wide range of matters, and have the potential to allow the grant of significant powers affecting the rights of individuals and other bodies…
>
> We take the view that the [Foreign and Commonwealth Office] has not provided sufficient justification for the delegation of powers by [the relevant portion of the act], particularly having regard to their wide scope and the significance of the powers conferred. Accordingly we consider the delegation of powers by [the relevant portion of the act] to be inappropriate.[55]

[54] Legislative and Regulatory Reform Act 2006 c. 51, *available at* https://www.legislation.gov.uk/ukpga/2006/51/pdfs/ukpga_20060051_en.pdf.
[55] Delegated Powers and Regulatory Reform Committee, "Seventh Report," Session 2017-19, HL paper 38 (Nov. 17, 2017) https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/38/3802.htm.

We agree entirely with the concerns of the Delegated Powers Committee; the Sanctions and Money Laundering Act of 2018 fails to establish any meaningful limiting principle in law that would cabin the authority of HM Treasury to surveil UK citizens or censor their communications. Nor does the Act establish any form of case-by-case adjudication or particular suspicion requirement that could ensure that surveillance is subject to the rule of law.

Conclusion

HM Treasury should keep in mind that basic rights to privacy and speech cannot be constitutionally abridged through arbitrary or extra-legal processes. The Sanctions and Money Laundering Act of 2018 lacks any specific and perspicuous statement of the law and process that must be followed when the rights of UK citizens are at stake. Because of that omission, the Act itself—secondary legislation aside—may be unconstitutional under the ICCPR and the ECHR. We do not press that argument in this comment. However, we urge HM Treasury to avoid proposing any secondary legislation that would facially restrict the speech and privacy rights of UK citizens by extending money laundering obligations to open-source software developers and others who may facilitate the use of cryptoassets but who do not take custody of cryptoassets on behalf of customers. Accordingly, we urge the UK to transpose 5MLD without augmentation, and—should any gaps remain—limit all further scope expansions to achieving parity with FinCEN's reasonable interpretation of the BSA.