



Stanford – Vienna Transatlantic Technology Law Forum



A joint initiative of
Stanford Law School and the University of Vienna School of Law

Transatlantic Antitrust and IPR Developments

Bimonthly Newsletter

Issue No. 1/2021 (April 16, 2021)

Contributors:

**Fernando Morera, Gabor Szecsi,
Marie-Andrée Weiss, Mauritz Kop, Pratyush Nath Upreti**

Editor-in-chief: Juha Vesala

Contents

- INTELLECTUAL PROPERTY 5**
- United States 5**
 - Who owns the copyright on Jack Ryan? 5
- European Union 13**
 - European Commission Action Plan on Intellectual Property 13
- OTHER DEVELOPMENTS 15**
- European Union and United States 15**
 - Central Bank Digital Currencies – Recent Transatlantic Developments 15
 - Democratic Countries Should Form a Strategic Tech Alliance 35
 - How to Ensure National Security in the New Media Age 50

About the contributors

Fernando Morera is an international tax attorney, currently working at Ernst & Young LLP (EY) in New York. His practice focuses on tax planning and consulting for private sector clients in the technology, retail, and financial sectors, as well as governments, and international organizations. He is also a member of EY's Advanced Technology Tax Lab, where he helps shape, lead, and implement open innovation initiatives, focused on developing open-source technology to build more resilient tax systems and societies around the world. Before joining EY, he was an NYU International Tax Fellow at the International Monetary Fund, where he contributed to legal policy making in the area of taxation of non-performing loans. He practiced tax and business law for several years in leading Argentine law firms, prior to moving to the United States in 2015. Fernando holds an LL.M. in International Taxation from New York University School of Law, as well as a J.D. (magna cum laude) and a B.S. in Accounting, both from the University of Buenos Aires, Argentina. He has been featured in Tax Notes International and Thomson Reuters, and is the author of more than thirty publications, including books and articles, on a wide range of international tax matters. Fernando has been a TTLF Fellow since September 2020.

Gabor Szecsi is a Hungarian American attorney licensed to practice law in California. He graduated from Karoli Gaspar University, Hungary, in 2007. During his PhD studies, he was an assistant professor of law in Hungary. He also graduated from the University of San Francisco Law School with an LL.M. in International Transactions and Comparative Law. He is an attorney in California, and his practice focuses on corporate transactions that include corporate law, securities law, company formation, shareholder rights, M&A deals, fund formation, and fund management. Gabor spent five years with the Hungarian office of the European Space Agency's Technology Transfer and Business Incubator Program, where he gained expertise in advising emerging aerospace and defense startups on various business and regulatory issues, including export-control and ITAR. His primary research interests include technology innovation, cross-border transactions, and market regulation. Gabor has been a TTLF Fellow since February 2021.

Marie-Andrée Weiss is an attorney admitted in New York and in Strasbourg, France. Before becoming an attorney, she worked for several years in the fashion and cosmetics industry in New York as a buyer and a director of sales and marketing. She graduated from the University of Strasbourg in France with an M.A. in Art History, a J.D. in Business Law, an LL.M. in Criminal Law, and an LL.M. in Multimedia Law. Marie-Andrée also graduated from the Benjamin N. Cardozo School of Law in New York City with an LL.M. in Intellectual Property Law. She is an attorney in New York and her solo practice focuses on intellectual property, privacy, data protection, and social media law. As a TTLF Fellow, Marie-Andrée's fields of research are freedom

of speech on social media sites and the use of consumers' likenesses in marketing and advertising.

Mauritz Kop is a Stanford Law School TTLF Fellow, Founder of MusicaJuridica and strategic intellectual property lawyer at AIRecht, a leading 4th Industrial Revolution technology consultancy firm based in Amsterdam. His work on regulating AI, machine learning training data and quantum technology has been published by Stanford, Harvard and Yale scholarly journals. Mauritz delivered copyright expertise to the European Parliament during the EU Copyright Directive legislative process. He held IP, music and technology law guest teaching positions at Leiden University, Maastricht University and Utrecht University and provided postdoc legal training to Supreme Court judges, lawyers and legal professionals at Radboud University. Mauritz is a member of the European AI Alliance (European Commission), the Dutch Copyright Society (VvA), CLAIRE (Confederation of Laboratories for Artificial Intelligence Research in Europe), the Dutch AI Coalition (NL AIC) and the ECP|Platform for the Information Society. He is author of numerous articles and blogs about legal and ethical aspects of exponential innovation in industrial sectors such as health-care, agrifood, and entertainment & art, and is a frequently asked international conference speaker on topics in the nexus of AI and Law. His present cross-disciplinary, comparative research focuses on human-centered AI, quantum-ELSI and sustainable disruptive innovation policy pluralism.

Pratyush Nath Upreti is a lawyer admitted to the Nepal Bar Council. He holds a research position at the Faculty of Law, University of Helsinki and also a research affiliate at Sciences Po Law School, Paris. Previously, he worked as a researcher at the Max Planck Institute for Innovation and Competition in Munich, Germany and a visiting researcher at the Centre for Intellectual Property Policy & Management (CIPPM) of Bournemouth University in the UK. He has taught Intellectual Property and International Trade Law at the Europe-North America and the Europe-Asia Programs of Sciences Po. Pratyush also serves as a member on the editorial board for the Global Trade and Customs Journal published by Kluwer Law International. He earned his PhD from Sciences Po, Paris and an LL.M. degree from Maastricht University, Netherlands as a UM High Potential Scholar. His interests include Intellectual Property Law, International Investment Law, and WTO related issues. He has been a TTLF Fellow since June 2018.

Intellectual Property

United States

Who owns the copyright on Jack Ryan?

By Marie-Andrée Weiss

On 10 February 2021, United States District Judge Ellen L. Hollander from the Federal District Court of Maryland published an 89-page Memorandum Opinion, addressing the issue of ownership of the books and fictional characters created by Tom Clancy, including Jack Ryan. The case is [Alexandra Clancy v. Jack Ryan Enterprises, Ltd.](#)

Facts

The character of Jack Ryan first appeared in *The Hunt for Red October (The Hunt)*, the first book ever published by Tom Clancy. It was published in 1984, by a small academic press, the United States Naval Institute (USNI). One of the book's characters is Jack Ryan, an analyst working for the Central Intelligence Agency. Jack Ryan became a recurring character in Tom Clancy's books, and appeared in several movies and television series adapted from Clancy's best-sellers.

Clancy and USNI signed a publishing agreement in 1983, which stated that:

“Author [Tom Clancy] grants and assigns to the Publisher [USNI] the exclusive worldwide rights and any subsisting copyright, including the right to secure copyrights and any renewals or extensions thereof, in connection with a certain unpublished work provisionally entitled THE HUNT FOR RED OCTOBER...” and also stated *“The Author agrees that he will not, without the written permission of the publisher, publish or permit to be published any material based on, or derived from, or directly competitive with the Work [i.e., Hunt], so long as this agreement shall remain in force.”*

On October 29, 1984, USNI received a certificate of copyright registration for *The Hunt* which identifies Clancy as the author, and USNI as the copyright claimant. On May 7, 1985, USNI, as owner of the exclusive rights, licensed a theatrical film from Paramount Pictures.

Jack Ryan Enterprises, Ltd. (“JREL”) was formed on May 28, 1985 by Tom Clancy and then-wife Wanda King. JREL's only assets were the computers that Clancy used to write his books. JREL was owned 40% by Tom Clancy, 40% by Wanda King, and 20% by their four children. Tom Clancy died in 2013, and JRE is now owned 40% by his estate, 40% by Wanda King, and 20% by Clancy and King's children. Wanda King is JREL's President.

The issue of ownership of the Jack Ryan character first arose between Clancy and

USNI in 1987. Clancy asked USNI to transfer the copyright registration for *The Hunt* back to him, claiming it was needed for Clancy to move forward with his negotiations with Viacom. USNI claimed it owned the rights to *The Hunt*.

Robert Youdelman, Clancy's attorney, told his client at the time that he believed that USNI had "acquired the copyright in [Hunt]," which gave it a continuing "interest in new books using the same characters." He added that "[t]he author of a novel usually retains the copyrights.... The publisher customarily has no interest in new books using the same characters," and noted that USNI had acquired "world-wide publishing rights" and added that because the "contract entitles [USNI] to 50% of all you make from any book in which 'Jack Ryan' or other characters from *Red October* appear, it is our view that this alone departs so far from industry practice as to make the entire contract unconscionable."

In 1988, Clancy filed for arbitration with the American Arbitration Association, arguing that he owned the Jack Ryan character, because the history of the relationship between USNI and Clancy showed that Clancy never relinquished his ownership of the now famous character. The parties settled: Clancy agreed to pay USNI \$125,000 and, in exchange, USNI agreed to reassign the copyright in *The Hunt* to Clancy. However, the agreement did not explicitly mention the Tom Clancy character.

JREL and Paramount entered into an agreement in 1989 clarifying the ownership

rights to the motion picture, television, and literary rights in *The Hunt*, which stated that JREL, as owner, had rights reserved for use and disposition, including in all literary property using the character Jack Ryan or any other principal character in *The Hunt*. JREL subsequently entered into other contracts for novels and movies featuring Jack Ryan.

Clancy formed Jack Ryan Limited Partnership ("JRLP"), a Maryland limited partnership, on 26 February 1992. Clancy's 50% interest is now owned by his estate. Regina King still owns 50%. In 1992, and again in 1994, Clancy entered into employment agreements with both JREL and JRLP.

Clancy formed Rubicon, Inc. in November 1995, which was owned entirely by Clancy. Clancy published *The Bear and the Dragon* (2000), *Red Rabbit* (2002), and *The Teeth of the Tiger* (2003), featuring Jack Ryan, under contracts executed by Rubicon. Clancy published these books without the agreement of the JR Entities and no proceeds were paid to the JR entities.

Clancy & King separated in November 1996. Their separation agreement included sections on the ownership and control of JREL and JRL:

"Husband [i.e., Clancy], Wife [i.e., King] and Michelle Clancy [one of the Older Children] are the only directors of JREL. Husband is the President, and Wife is the Vice President, Treasurer and Secretary of JREL + Clancy, as president of JREL, would have the usual powers of the chief executive of a personal service corporation, including the

power to negotiate and sign on behalf of JREL royalty and other contracts..."

This agreement was incorporated in the 1999 divorce decree. Tom Clancy married Alexandra Clancy in 1999. The couple stayed married until Clancy's death in October 2013 and had one child.

Paramount announced in 2008 that it was developing a new movie, *Jack Ryan: Shadow Recruit*, featuring Jack Ryan, which would not be based on any of Clancy's previous novels. Based on emails between Clancy and his representatives, there was some concerns on whether Paramount had the right to develop the Jack Ryan character. Robert Youdelman reminded Clancy's agent that the "*Jack Ryan' character is owned by Jack Ryan Enterprises Ltd, an entity in which Wanda [King] and the children have an interest[.]*" Paramount eventually paid to use the Jack Ryan character in the new movie.

Clancy died in 2013. After his death, Putnam wanted to publish "Tom Clancy" novels, at least one novel focusing on the Jack Ryan character. In March 2015, his Estate, Rubicon, JREL, and JRLP, collectively as the "Author," executed a four-book deal with Putnam.

Procedure

Alexandra Clancy filed on August 25, 2017 a complaint for declaratory judgment in the Circuit Court for Baltimore City to obtain a declaration that the rights to the Jack Ryan

character are owned by Rubicon, a company created by Tom Clancy, which is now wholly-owned by the Tom Clancy Estate.

Defendants are J.W. Thompson Webb, as personal representative of the Estate of Thomas L. Clancy, Jr. (the "Estate") and the three separate business entities formed by Clancy: JREL, JRLP and Rubicon.

The case was removed to the federal District Court for the District of Maryland because some of the claims arise under the Copyright Act.

Authorship and Work Made for Hire

Defendants claim that JR Books were written as works made for hire for the JR Entities, which, therefore, own all of the copyrightable elements of the books, including the characters delineated in them.

Neither side argues that any of the books were "specially ordered or commissioned," and thus the issue is whether Clancy was an employee of the JR Entities and wrote the JR Books within the scope of his employment.

If Clancy was an employee of JREL and JRLP, then the works he wrote at the time are works for hire and the two companies own the copyright. This is the view of the Defendants, but not, of course, of the Plaintiff, who claims that Clancy was neither an employee nor agent of the JR Entities, that, therefore, the works are not works made for hire as Clancy's relationship with the JR

Entities “*had none of the earmarks of a true employee relationship.*”

[Section 101 of the Copyright Act](#) defines a work for hire as:

“(1) a work prepared by an employee within the scope of his or her employment; or

(2) a work specially ordered or commissioned for use as a contribution to a collective work, as a part of a motion picture or other audiovisual work, as a translation, as a supplementary work, as a compilation, as an instructional text, as a test, as answer material for a test, or as an atlas, if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire.”

The Copyright Act does not define the terms “employee” or “employment,” however, leaving the application of the terms to the courts.

The U.S. Supreme Court held in [Community for Creative Non-Violence v. Reid](#), that “*the term ‘employee’ should be understood in light of the general common law of agency,*” and set out a non-exhaustive list of factors to consider. However, none of these factors are determinative, and the Supreme Court did not indicate how the factors must be weighed.

The Courts do not mechanically apply the *Reid* factors and only consider the factors which are relevant in each case:

- hiring party’s right to control the manner and means by which the product is accomplished;
- skill required;
- source of the instrumentalities and tools;
- location of the work;
- duration of the relationship between the parties;
- whether the hiring party has the right to assign additional projects to the hired party;
- extent of the hired party’s discretion over when and how long to work;
- method of payment;
- hired party’s role in hiring and paying assistants;
- whether the work is part of the regular business of the hiring party;
- whether the hiring party is in business;
- provision of employee benefits; and
- tax treatment of the hired party

The Second Circuit Court of Appeals identified in [Aymes v. Bonelli](#) five factors to consider when determining whether a work was made for hire:

- hiring party's right of control over the hired party;
- skill required of the hired person;
- provision of employee benefits;
- tax treatment of the hired party; and
- whether the hiring party has the right to assign additional projects to the hired party.

Judge Hollander found the *Aymes* factors "*particularly relevant*" in the *Clancy* case, and concluded that they weighed against finding a work for hire status, as evidence demonstrated that neither of the JR Entities had attempted to "*control the manner and means*" by which Clancy's books were written. King acknowledged that Clancy had complete autonomy with respect to every aspect of his books, and even though she may have reviewed the books once they were written, it was Clancy who chose what books to write and when to work on them.

Clancy was a co-owner of both entities, but there are factors that support finding that the famous author was an employee of the JR Entities:

- JREL paid for the computer that Clancy used to write the books;
- Clancy worked for both entities for an extended period of time;
- Clancy's work was part of the regular business of the entities; and

- Clancy received health benefits.

Defendants argued that publishing agreements between the JR Entities and Putnam proved that Clancy believed the books were made for hire. Judge Hollander found that these agreements prove that Clancy had the intent to form an employment relationship, but that they did not necessarily "*suffice on [their] own*" to overcome the factors weighing against finding a work for hire relationship.

Judge Hollander could not thus conclude, as a matter of law, that Clancy was an employee of the JR Entities and that his books were made for hire and denied both Plaintiff and Defendants' motions with respect to the work for hire claims.

Alleged Copyright Assignments from Clancy to the JR Entities

The Parties did not dispute that JREL owns the copyright to *The Hunt* but disagreed over whether the Jack Ryan character as developed in *The Hunt*, was assigned to USNI and then JREL, along with the copyright in *The Hunt* or, instead, whether Clancy retained the copyright in Jack Ryan at the time of his death.

Ownership of a copyright is freely transferable "*by any means of conveyance or by operation of law,*" [17 U.S.C. § 201\(d\)\(1\)](#). However, "[a] *transfer of ownership, other than by operation of law, is not valid unless an instrument of conveyance, or a note or a memorandum of the transfer, is in writing*

and signed by the owner of the rights conveyed or such owner's duly authorized agent," [17 U.S.C. § 204\(a\)](#).

Section 204's requirement may be satisfied by an oral assignment that is subsequently ratified or confirmed by a written memorandum of the transfer.

Defendants claimed that JR Entities own the JR Books and their characters because the copyrights were validly assigned to them by Clancy, pursuant to 17 U.S.C. § 204(a), while Plaintiff claims that any alleged assignment of the JR Books to the JR Entities was ineffective.

Defendants argued that there were "*several written instruments, signed by Tom Clancy, that memorialize the transfer of copyright in each book from Tom Clancy to JREL and JRLP, respectively,*" including:

- the publishing agreements with Putnam;
- the Guaranty Letters accompanying those agreements;
- the Separation Agreement that acknowledges ownership of the books by JREL and JRLP;
- Guaranty Letters and the Separation Agreement operate as written "*note[s] or memorandum[a]*" validating earlier transfers between the JR Entities and Clancy.

Plaintiff argued that these are not the kind of documents that "*qualify as assignments*" under Section 204 and that "*none of the referenced documents are between Clancy*

and JREL or JRLP," none of them "*set forth the clear and unequivocal intent to transfer required by Section 204.*"

Judge Hollander applied Maryland law to interpret the agreements and concluded Tom Clancy clearly intended to transfer copyright ownership to the JR Entities, and that the requirement of an assignment under Section 204(a) were satisfied.

Impact of the assignment on ownership of the characters featured in the JR Books, including Jack Ryan

Judge Hollander noted that the parties appeared to agree that the owner of the copyright to these works also owns the rights to the characters or the incremental character developments in them, with the exception, however, of the Jack Ryan character. She considered separately the issue of ownership of the Jack Ryan character and concluded that the characters developed in the JR Books, like the books themselves, were validly assigned to the JR Entities.

The parties disagreed on whether the assignment to USNI of the copyright to *The Hunt*, and the assignment of *The Hunt* to JREL included assignment of the copyright in Jack Ryan, a character who first appeared in this book.

Defendants claimed that Clancy assigned the copyright in *Hunt* to USNI "*without reservation,*" and thus USNI acquired the copyright to the Jack Ryan character, and that, when USNI assigned the copyright in *The*

Hunt to JREL, "it also assigned the rights to Jack Ryan as delineated in Hunt to JREL."

Plaintiff stated that Jack Ryan "is a fully delineated, distinctive and iconic character," and is "important to the Clancy franchise." She conceded that the rights to *The Hunt* were assigned to USNI and JREL, but not the character of Jack Ryan:

"The 1983 [USNI] Contract does not grant USNI any rights to the characters featured in HUNT or to sequels or derivative works. None can be inferred."

Fictional characters are not an enumerated copyrightable subject matter under the Copyright Act, see [17 U.S.C. § 102\(a\)](#), but [courts recognized](#) that they can be protected by copyright if developed with enough specificity so as to constitute protectable expression.

The Ninth Circuit Court of appeals explained, however, in [DC Comics v. Towle](#), that "[n]ot every comic book, television, or motion picture character is entitled to copyright protection." The Ninth Circuit enumerated its "Towle" test for characters:

A character is entitled to copyright protection if

- the character has "physical as well as conceptual qualities;"
- the character is "sufficiently delineated to be recognizable as the same character whenever it appears" and "display[s] consistent, identifiable character traits and attributes;" and

- the character is "especially distinctive" and "contain[s] some unique elements of expression."

[Section 201\(d\)\(2\) of the Copyright Act](#) provides:

Any of the exclusive rights comprised in a copyright, including any subdivision of any of the rights specified in section 106, may be transferred...and owned separately. The owner of any particular exclusive right is entitled, to the extent of that right, to all of the protection and remedies accorded to the copyright owner by his title.

As such, under the theory of divisible copyrights, fictional characters may be protected separately from the underlying work, and this copyright may be assigned separately from the copyright in the general work.

Judge Hollander noted that the issue was not only whether Jack Ryan was sufficiently delineated in *The Hunt* to be protected by copyright, separately from the book, but also whether the assignments of *The Hunt* copyright to USNI, then JREL, included the transfer of ownership of Jack Ryan.

As both parties agreed that Jack Ryan is sufficiently developed to be protected, Judge Hollander addressed only the issue of assignment of rights, found these assignments to be ambiguous and denied summary judgment:

"Whether the rights to Jack Ryan were assigned to USNI or JREL, as part of the assignment of rights to Hunt, depends on the interpretation of the... agreements.

...Applying the tools of contract interpretation, I conclude that the assignment of rights to Jack Ryan is ambiguous because at least one of the relevant agreements—the Settlement Agreement—is susceptible to multiple interpretations.”

The case is now heading to trial. A jury will be asked to decide who owns the Jack Ryan character, unless the parties settle.

Intellectual Property

European Union

European Commission Action Plan on Intellectual Property

By Pratyush Nath Upreti

On 25 November 2020, the European Commission adopted a new '[Action Plan on Intellectual Property](#)' for the EU recovery and resilience. The action plan reaffirms intellectual property as a key driver to economic growth in the European Union. The action plan is drafted keeping in mind the impacts that Covid-19 may have on innovators and small and medium-sized enterprises (SMEs).

Challenges

Generally, the action plan aims to ensure that innovators have access to fast, effective, and affordable means to protect their intangible capitals. The action plan identifies five challenges that EU companies are facing in protecting their intangible capital; (i) fragmentation in the EU's IP system (ii) SMEs lack of adequate use of opportunities offered by IP protection (iii) insufficient development of tools to facilitate access to IP

(iv) counterfeiting and piracy still thriving and (v) lack of fair play at the global level.

Focus areas of intervention

The action plans emphasize ensuring fast, effective and affordable protection tools to innovators. To do so, the Commission has prioritized three improvements on IPRs protection: (i) Commission argues for the rapid roll-out of the unitary patent system (ii) optimize the supplementary protection certificates system (iii) reforming industrial design to meet the support the digital and green economy (iv) improving the EU geographical indications system with the prospects of extending protection for non-agricultural products. Another focus area that Commission aims to address is the EU's capacity to innovate by encouraging innovators and creators to utilize opportunities that IP provides. This is done by incentivizing innovators by introducing IP vouchers for SMEs hit by the Covid-19 crisis. Similarly, financial support and help in managing SME's IP portfolios are some short-term plans.

Access and Sharing of IP protected assets

The action plan emphasizes developing better licensing tools to facilitate access to IP in times of crisis. The Commission acknowledges the [World Health Organization \(WHO\) Resolution in response](#) to the COVID-19 crisis and reaffirms the relevance of 'voluntary pooling and licensing of

IP related to COVID-19 therapeutics and vaccines' pursuant to WHO Resolution. Additionally, the Commission recognises the need for an 'effective system for issuing compulsory licenses, but as 'a means of last resort... when all other efforts to make IP available have failed'.

Concerning standard-essential patents (SEPs), the commission will focus on reforms on clarifying and improving the framework on governing, licensing, and enforcement of SEPs. Similarly, the Commission commits to promoting data sharing in line with [European Strategy for Data](#).

Fighting Infringements and Global Fair play

To address the concerns of online platforms, the Commission commits to 'clarify and upgrade the responsibilities of online platforms' and improve the capacity of law enforcement authorities. Similarly, to overcome the counterfeit and piracy challenges, the Commission plans to establish the 'EU Toolbox against counterfeiting' to promote the use of new technologies such as artificial intelligence, image recognition and blockchain.

Finally, the action plans demonstrates the Commission's continuous interest in IP chapters of free trade agreements to ensure higher standards of IP protection for EU business. Similarly, to protect the brands, the Commission commits to EU accession

to the [Singapore Treaty on the Law of Trademarks](#).

Other Developments

European Union and United States

Central Bank Digital Currencies – Recent Transatlantic Developments

By *Fernando Morera*¹

This report takes stock of recent developments in the area of Central Bank Digital Currencies (“CBDC”) in the European Union (“EU”) and the United States (“US”), focusing on select design, central bank law, and monetary law considerations. A forthcoming paper² will analyze, in greater detail, these and other legal matters (e.g., under tax law and data privacy and protection

law), while providing a more robust point of view around design, technology, policy, and behavioral aspects of CBDC initiatives in the EU, the US, and the United Kingdom.

This report is structured in four sections. Section one discusses basic monetary and legal concepts to help contextualize the CBDC discussion. Section two reviews recent CBDC developments in the EU and, more specifically, in the euro area.³ Section three covers recent CBDC developments in the US. Section four highlights some take-aways of this preliminary analysis.

1. Background

a. About money

To understand CBDC and their potential implications, it is useful to briefly discuss what money is and how it is created. Money has taken multiple forms throughout history. Early forms of money involved *commodity money* – i.e., an object made of a given material, like gold or silver, with market value.⁴

¹ © Fernando Morera 2021 (all rights reserved). Fernando is a Transatlantic Technology Law Forum Fellow at Stanford Law School. His research focuses on Governance Innovation, exploring novel governance models for business ecosystems, open innovation, and emerging technologies. He holds an LL.M in International Taxation from New York University (NYU) School of Law, as well as a J.D. (*magna cum laude*), and a B.S in Accounting (*equivalent*), both from the University of Buenos Aires, Argentina. Fernando was an NYU International Tax Fellow at the International Monetary Fund in 2016. The views or opinions expressed in this report are those of the author and do not necessarily reflect the views or opinions of other people or organizations.

² Fernando Morera, “Central Bank Digital Currencies – A Transatlantic Perspective”, TFLF Working Paper Series (forthcoming). See abstract here: <https://law.stanford.edu/projects/central-bank-digital-currencies-a-transatlantic-perspective/> (last accessed February 27, 2021).

³ The euro area includes EU member countries that have adopted the euro as their currency. See “What is the euro area?” at: https://ec.europa.eu/info/business-economy-euro/euro-area/what-euro-area_en (last accessed March 14, 2021).

⁴ See “What is Money” at https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.en.html#:~:text=The%20uses%20of%20money%20and%20how%2

Later on, money became *representative money*, which primarily consisted of banknotes or other physical tokens, redeemable in gold or silver.⁵ Today, money is largely *fiat money*, which is not redeemable for gold, silver or assets, but is generally trusted as a valid means of payment to settle debts.⁶

Fiat money can be physical or electronic. Physical money is normally currency. Currency generally comprises banknotes and coins.⁷ Currency bears no interest and can only be issued by central banks.⁸ Currency is a liability for central banks and an asset for its holders – i.e., banknotes and coins are physical tokens carrying a promise to pay to their holders.⁹ Electronic money comes in two main forms – central bank reserves and commercial bank deposits.

[0the%20ECB%20keeps%20track%20of%20it&text=It%20is%20a%20medium%20of,is%20a%20store%20of%20value](#) (last accessed March 13, 2021).

⁵ Id.

⁶ Id.

⁷ Bank of England, “Money in the modern economy: an introduction”, Quarterly Bulletin 2014 Q1, p. 8.

⁸ Id., p.8.

⁹ Wouter Bossu; Masaru Itatani; Catalina Margulis; Arthur D. P. Rossi; Hans Weenink; Akihiro Yoshinaga, “Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations”, IMF Working Paper No. 2020/254, p. 11. Available at: <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827> (last accessed February 28, 2021).

¹⁰ Bank of England, “Money in the modern economy: an introduction”, Quarterly Bulletin

Central bank reserves are electronic records of the amount owed by central banks to depositary institutions, such as commercial banks.¹⁰ They represent liabilities for central banks and assets for commercial banks.¹¹ It is useful to think of central bank reserves as deposits held by commercial banks with central banks –similar to deposits that households or businesses hold with commercial banks, which are further explained below. Central bank reserves, however, can only be accessed by commercial banks through master accounts held with central banks.¹² These master accounts are used to carry out wholesale transactions between commercial banks¹³, very much like households or businesses use their commercial bank accounts to undertake retail operations with their counterparties.¹⁴ Central bank reserves are also known as

2014 Q1, p. 11. Available at:

<https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-in-the-modern-economy-an-introduction> (last accessed March 14, 2021).

¹¹ Id., p. 11. See also Figure 2 on page 8 depicting stylized balance sheets of different type of money holders and issuers in the economy. There, central bank reserves are listed as liabilities for central banks; representing assets for commercial banks.

¹² See the definition of “master account” here: <https://www.frbservices.org/financial-services/accounting/service-setup/master-account.html> (last accessed March 13, 2021).

¹³ They are wholesale operations because of their large volume, and because they are generally undertaken by commercial banks or other big players in the market, with support of central banks.

¹⁴ Retail banking, by contrast, generally focuses on smaller-scale operations with

the *ultimate asset* of commercial banks to settle payments – i.e., banking transactions between commercial banks' customers are directly or indirectly settled through transfers between master accounts held by commercial banks at central banks.¹⁵ Central bank reserves also generally bear interest, payable by central banks to commercial banks.¹⁶

Commercial bank deposits, in turn, are an electronic record of the amount owed by commercial banks to their retail clients – e.g., individuals, households and businesses. Bank deposits are created by commercial banks and not by central banks.¹⁷ Bank deposits come in different forms, such as current or checking accounts, or saving accounts.¹⁸ They represent liabilities for commercial banks and assets for their clients.¹⁹ The stock of bank deposits generally grows as banknotes or coins are paid to, or deposited into, bank accounts held by customers.²⁰ The stock decreases with every withdrawal.²¹ This stock is also

influenced by inbound and outbound wire transfers into, and from, those accounts. To respond to withdrawal requests from clients, commercial banks generally maintain a minimum stock of cash in their vaults. In most modern and advanced economies bank deposits are normally the default type of money and clients tend to use them widely to settle their obligations²², without converting them into cash. Bank deposits also bear interest, payable by commercial banks to their customers.

The vast majority of the money circulating in the economy is created by commercial banks.²³ Their ability to create money is not unlimited and is typically regulated by central banks. Some argue, however, that this ability is weakly linked to the volume of reserves commercial banks hold at central banks.²⁴ Commercial banks create money primarily by granting loans to their customers.²⁵ Loaned balances are generally deposited in their customers' accounts.²⁶ Loans are therefore assets for commercial

individual clients, households, and small- or mid-size businesses.

¹⁵ Bank of England, "Understanding the central bank balancesheet", 2015, p. 10. Available at: <https://www.bankofengland.co.uk/-/media/boe/files/ccbs/resources/understanding-the-central-bank-balance-sheet.pdf> (last accessed March 14, 2021).

¹⁶ See, for instance "Interest on Required Reserve Balances and Excess Balances" paid by the US Federal Reserve Banks to depository institutions at: <https://www.federalreserve.gov/monetarypolicy/regresbalances.htm> (last accessed March 13, 2021).

¹⁷ Bank of England, "Money in the modern economy: an introduction", Quarterly Bulletin 2014 Q1, p. 11. Available at: [https://www.bankofengland.co.uk/quarterly-](https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-in-the-modern-economy-an-introduction)

[bulletin/2014/q1/money-in-the-modern-economy-an-introduction](https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-in-the-modern-economy-an-introduction) (last accessed March 14, 2021).

¹⁸ Id., p. 10.

¹⁹ Id., p. 11. See also Figure 2 on page 8.

²⁰ Id., p. 11.

²¹ Id., p. 11.

²² Id., p. 11.

²³ Josh Ryan-Collins, Tony Greenham, Richard Werner, Andrew Jackson, "Where Does Money Come From – A Guide to the UK Monetary and Banking System", New Economics Foundation, 2012, p. 7

²⁴ Id., p. 7.

²⁵ Id., p. 7.

²⁶ Bank of England, "Money in the modern economy: an introduction", Quarterly Bulletin 2014 Q1, p. 11. Available at:

banks and liabilities for their customers.²⁷ Loans normally bear interest, payable by customers to their commercial banks. Interest charged on loans is normally higher than interest paid on bank deposits, and this is how commercial banks have historically earned income.²⁸ Once customers pay their loans in full, that commercial bank money ceases to exist – i.e., it is cancelled.

In the process of money creation and intermediation, central banks support commercial banks in several ways. For instance, central banks **(i)** allow commercial banks to settle interbank payments using central bank reserves; **(ii)** enable convertibility between commercial and central bank money through banknote provision; and **(iii)** and function as lenders of last resort, in case commercial banks are in need of liquidity.²⁹

Central banks influence the amount of money, of all kinds, circulating in the economy through specific tools of monetary policy, such as interest rates, and reserve

requirements. In theory, central banks can leverage these tools to control the amount of credit that commercial banks can issue to their clients. For example, they may set higher interest rates on loans to restrict demand of money and therefore reduce the amount of credit circulating in the economy. Some argue, however, that given the oversized role that commercial banks play in the creation of money, in actuality, they are the ones who influence how much central bank reserves are needed to keep the system functioning properly.³⁰

b. Conceptualizing money

The concept of money is continually evolving. In addition to currency, central bank reserves, and bank deposits discussed above, some argue that money also includes digital cash or e-money – i.e., monetary value stored in a pre-paid credit card or smartphones.³¹ Further, digital currencies, such as Bitcoin, may be considered money by some parties³², but not by others.³³ The

<https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-in-the-modern-economy-an-introduction> (last accessed March 14, 2021).

²⁷ *Id.*, p. 8, figure 2.

²⁸ Needless to say, this is an overly simplified representation of their business model and does not factor in a wide range of other banking operations.

²⁹ BIS, “Central bank digital currencies: foundational principles and core features”, October 9, 2020, p. 4. Available at: <https://www.bis.org/publ/othp33.htm> (last accessed March 8, 2021).

³⁰ Josh Ryan-Collins, Tony Greenham, Richard Werner, Andrew Jackson, “Where Does Money Come From – A Guide to the UK Monetary and

Banking System”, New Economics Foundation, 2012, p. 7.

³¹ See “What is money?” at https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.en.html#:~:text=The%20uses%20of%20money%20and%20how%20the%20ECB%20keeps%20track%20of%20it&text=It%20is%20a%20medium%20of,is%20a%20store%20of%20value. (last accessed March 13, 2021).

³² *Id.*

³³ Yves Mersch, “Virtual or virtueless? The evolution of money in the digital age”, Lecture delivered at the Official Monetary and Financial Institutions Forum, London, February 8, 2018. Available at: <https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180208.en.html#footnote.2> (last accessed March 14,

reality is that there is no single, commonly accepted definition of money across all areas of knowledge. Each discipline has a rather *sui generis* approach to this matter.

For example, from a legal perspective, in most countries, money generally means: (i) cash (i.e., banknotes and coins); (ii) central bank reserves; and (iii) commercial bank deposits.³⁴ The legal definition of money, in turn, is closely linked to two legal constructs. The first one is the concept of *currency*. Legally, currency refers to the official means of payment of any given jurisdiction, which is recognized as such under monetary law.³⁵ Most monetary laws grant currency status to both banknotes and coins.³⁶ Others, however, appear to grant currency status only to banknotes, treating coins as a seemingly different category of money.³⁷

2021). See, in particular, the chapter “What is money?”, where the author sustains that digital currencies are not money because they generally do not function as (i) unit of account; (ii) medium of exchange; and (iii) store of value. The author focuses on the economic definition of money, which is also explored in this report.

³⁴ Wouter Bossu; Masaru Itatani; Catalina Margulis; Arthur D. P. Rossi; Hans Weenink; Akihiro Yoshinaga, “Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations”, IMF Working Paper No. 2020/254, p. 8, Box 1. Available at: <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827> (last accessed February 28, 2021).

³⁵ *Id.*, p. 8, Box 1.

³⁶ *Id.*, p. 8, Box 1.

³⁷ In the US, for example, only banknotes seem to be considered currency, as suggested by section 5103 of the US Code, which

Legal tender is the second legal construct. Legal tender is what entitles debtors to settle their obligations by *tendering* currency, or other lawful means of payment, to their creditors.³⁸ Currency, by definition, has legal tender status.³⁹ But legal tender status can be extended to other means of payment⁴⁰ and include, for example, balances deposited in accounts held with commercial banks. As a result, even if a medium of exchange is not technically considered currency, it could have legal tender status, and be used to settle debts.

Interestingly, the recognition of money as legal tender normally applies in the narrow context of *debt settlement*, but does not necessarily extend to other transactions, where parties have the freedom to use other means of payment, as they see fit.⁴¹ This

refers to “*United States coins and currency*” as two, seemingly different concepts.

³⁸ Wouter Bossu; Masaru Itatani; Catalina Margulis; Arthur D. P. Rossi; Hans Weenink; Akihiro Yoshinaga, “Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations”, IMF Working Paper No. 2020/254, p. 8, Box 1. Available at: <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827> (last accessed February 28, 2021).

³⁹ *Id.*, p. 8, Box 1.

⁴⁰ *Id.*, p. 8, Box 1. Within the euro area article 128(1) of the Treaty on the Functioning of the European Union recognizes the legal tender status of euro banknotes. Articles 10 and 11 of the Council Resolution (EC) No. 974/98 do the same with respect to euro banknotes, while extending legal tender status to euro coins, as well.

⁴¹ See, for instance, the following statements:

implies that the use of money as a medium of exchange is largely a function of trust. Parties will generally use money, regardless of its legal tender status, if they believe it is a trustworthy means of payment.⁴²

From an economic perspective, the definition of money focuses on its functions. In general, money has three functions **(i)** unit of account⁴³; **(ii)** medium of exchange⁴⁴; and

(i) *“For example, Bank of England banknotes are the only notes that are legal tender in England and Wales. But that legal tender status only has a narrow meaning relating to the repayment of debts. In ordinary transactions it has little practical application, since whether a currency is used as the medium of exchange depends only on whether there is agreement between the two parties carrying out the exchange (emphasis added). See Bank of England, “Money in the modern economy: an introduction”, Quarterly Bulletin 2014 Q1, footnote 3. Available at: <https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-in-the-modern-economy-an-introduction> (last accessed March 13, 2021).*

(ii) In the euro area, *“this means that in the absence of an agreement of the means of payment, the creditor is obliged to accept a payment made in euro which subsequently discharges the debtor from his payment obligation. Yet, during transactions, contractual parties are free to use other official foreign currencies with legal tender status in the state of issuance (e.g., the pound sterling or the US dollar). The same applies to privately issued money like local exchange trading systems (e.g., voucher-based payment systems in certain communities) or virtual currency schemes (e.g., Bitcoin).”* See “Official Currency” at <https://ec.europa.eu/info/business-economy->

(iii) store of value.⁴⁵ Although there is some overlap between the legal and economic definitions of money⁴⁶, they do not perfectly match, proving the point that the concept of money is largely contextual.

As the US Supreme Court suggested in *Wisconsin Central*, what qualifies as money and, thus, as a valid medium of exchange “*may depend on the facts of the day.*”⁴⁷

[euro/euro-area/euro/use-euro/euro-legal-tender-en](https://www.bankofengland.co.uk/euro/euro-area/euro/use-euro/euro-legal-tender-en) (last accessed March 12, 2021).

(iii) United States coins and currency are legal tender for all debts. However, *“there is no federal statute which mandates that private businesses must accept cash as a form of payment. Private businesses are free to develop their own policies on whether or not to accept cash unless there is a State law stating otherwise.”* (emphasis added). See “Legal Tender: A Definition” at <https://www.moneyfactory.gov/resources/lawsandregulations.html> (last accessed March 12, 2021).

⁴² Bank of England, “Understanding the central bank balancesheet”, 2015, p. 5. Available at: <https://www.bankofengland.co.uk/-/media/boe/files/ccbs/resources/understanding-the-central-bank-balance-sheet.pdf> (last accessed March 14, 2021).

⁴³ Money allows goods and services to be priced. See “What is money?” at https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.en.html#:~:text=The%20uses%20of%20money%20and%20how%20the%20ECB%20keeps%20track%20of%20it&text=It%20is%20a%20medium%20of,is%20a%20store%20of%20value. (last accessed March 13, 2021).

⁴⁴ Money is a means of payment with a value that everyone trusts. See previously cited source.

⁴⁵ So that money can be saved, retrieved, and exchanged without significantly losing value.

⁴⁶ Unit of account and medium of exchange would overlap, to some extent, with the definition of currency and legal tender.

⁴⁷ *Wisconsin Central Ltd. v. United States*, 138 S. Ct. 2067 (2018), p. 10 of the majority

Justice Breyer, on his dissenting opinion, went even further, hinting that the definition of currency may one day include “*Bitcoin or some other type of cryptocurrency*.”⁴⁸ Below, we explore how CBDC would fit in the definition of money.

c. Conceptualizing CBDC

The progressive decline in the use of cash in certain economies, coupled with the proliferation of other digital currencies (e.g., cryptocurrencies and stablecoins), and the need to create more resilient payment systems, have propelled governments, in consultation with other actors, to actively study the merits of issuing CBDC.⁴⁹

The CBDC phenomenon is not new, however. It has been studied for over a decade by academics and activists.⁵⁰ Some argue that this concept is even older, going back to the 1980s, when James Tobin, an American Nobel Laureate in economics, suggested that Federal Reserve Banks in the US could make available to the public a widely accessible “*medium with the convenience of deposits and the safety of currency*,

opinion. Available at: https://www.supremecourt.gov/opinions/17pdf/17-530_6537.pdf (last accessed March 14, 2021).

⁴⁸ Id., p. 3 of Breyer’s dissenting vote.

⁴⁹ BIS, “Central bank digital currencies: foundational principles and core features”, October 9, 2020, p. 1. Available at: <https://www.bis.org/publ/othp33.htm> (last accessed March 8, 2021).

⁵⁰ See references in Ole Bjerg, “Designing New Money – The Policy Trilemma of Central Bank Digital Currency”, Copenhagen Business School, CBS Working Paper, June 2017, p. 10.

⁵¹ James Tobin, “The case for preserving regulatory distinctions”, in Proceedings of the

transferable in any amount by check or other order.”⁵¹

Albeit there is no commonly accepted definition of CBDC as of the date of this report⁵², it is generally understood that CBDC would be a form of *digital* money, intended to have both currency and legal tender status, which is issued, backed, and governed by central banks, and is ultimately a liability for them. CBDC would therefore be a form of central bank money.

CBDC are different from “synthetic CBDC”, “stablecoins”, and other digital currencies or assets. CBDC are issued as central bank liabilities, and have the features mentioned before. Synthetic CBDC or stablecoins involve other, non-central bank actors issuing liabilities matched by funds held at a central bank⁵³, or by other assets held elsewhere. CBDC are also different from other digital currencies or assets, like Bitcoin. Bitcoin, for example, is not backed by any asset, does not bear interest, and is not governed by any central party or authority.⁵⁴

Economic Policy Symposium, Jackson Hole, Federal Reserve Bank of Kansas City, 1987, p. 172.

⁵² This report was submitted for publication on March 20, 2021.

⁵³ BIS, “Central bank digital currencies: foundational principles and core features”, October 9, 2020, p. 4. Available at: <https://www.bis.org/publ/othp33.htm> (last accessed March 8, 2021).

⁵⁴ Antony Lewis, “The Basics of Bitcoins and Blockchains – An Introduction to Cryptocurrencies and the Technology that Powers Them”, Mango Publishing, 2018, p. 150.

Definitions aside, there is a heated debate around the world as to whether CBDC, if issued, will replace or complement other forms of money, and the potential monetary and economic implications of these choices.⁵⁵ Jurisdictions are also wrestling with other design-related questions, such as: (i) whether CBDC should be “account-based” (accessible through accounts)⁵⁶ or “token-based” (represented by digital tokens)⁵⁷; (ii) whether CBDC should be “retail” (widely accessible by the public, like cash), or “wholesale” (only accessible by commercial banks, like central bank reserves); and (iii) whether CBDC should leverage distributed ledger technology, or other technical innovations. These questions, along with broader legal, policy, technology, economic,

and behavioral ramifications of CBDC will ultimately determine if and how jurisdictions will move forward in this space.

Currently, there are several CBDC projects around the world, all of which have different degrees of development.⁵⁸ A recent survey conducted by the Bank of International Settlements (“BIS”) highlighted that central banks representing collectively a fifth of the world’s population are likely to issue a retail form of CBDC in the next three years.⁵⁹ The survey also highlighted that central banks in emerging markets and developing economies consider themselves more likely to issue a retail CBDC than their peers in advanced economies.⁶⁰

⁵⁵ For a conceptual and philosophical analysis of these implications, see Ole Bjerg, “Designing New Money – The Policy Trilemma of Central Bank Digital Currency”, Copenhagen Business School, CBS Working Paper, June 2017. Available at: <https://research.cbs.dk/en/publications/designing-new-money-the-policy-trilemma-of-central-bank-digital-c> (last accessed March 20, 2021).

⁵⁶ In an account-based system, the identity of the account holder has to be verified to gain access to CBDC. See Jesús Fernández-Villaverde Daniel Sanches, Linda Schilling, and Harald Uhlig “Central Bank Digital Currency: Central Banking For All”, Federal Reserve Bank of Philadelphia, August 2020. Available at: <https://www.philadelphiafed.org/consumer-finance/payment-systems/central-bank-digital-currency-central-banking-for-all> (last accessed March 2, 2021).

⁵⁷ In a token-based system, the validity of the payment object needs to be verified to gain access to CBDC. Also, under this system, the knowledge of a password would grant access to CBDC. For more details, see paper cited in the previous footnote. See also Wouter Bossu; Masaru Itatani; Catalina Margulis; Arthur D. P.

Rossi; Hans Weenink; Akihiro Yoshinaga, “Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations”, IMF Working Paper No. 2020/254, p. 11. Available at: <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827> (last accessed March 14, 2021).

⁵⁸ The Atlantic Council keeps track of them here: <https://www.atlantic-council.org/blogs/econographics/the-rise-of-central-bank-digital-currencies/> (last accessed March 13, 2021).

⁵⁹ BIS, “Ready, steady, go? – Results of the third BIS survey on central bank digital currency”, BIS Paper No. 114, January 2021. Available at: <https://www.bis.org/publ/bppdf/bispap114.htm> (last accessed March 14, 2021).

⁶⁰ Id., p. 11. Also, according to this survey, 65 central banks responded to the survey. Respondents represented approximately 72% of the world’s population and 91% of the global economic output. 21 respondents were located in Advanced Economies (AE) and 44 were in Emerging Market and Developing Countries

Yet very few central banks seem to be allowed to issue CBDC under their current legal frameworks. Staff at the legal department of the International Monetary Fund (“IMF”) reviewed the central bank laws of 174 member countries and found that only about 40 would be legally allowed to issue CBDC.⁶¹ According to this IMF publication, close to 80% of the world’s central banks are either not allowed to issue CBDC or their legal framework is not clear on this specific matter.⁶²

Given the strategic and geopolitical implications of CBDC, the US and the EU have developed a keen interest in progressing this agenda. Their approach, however, seems to be cautious, compared to that of other incumbents.⁶³ They both appear to agree on

(EMDE). See, in particular, graph 1 on page 5, and annex 1 on page 18.

⁶¹ Catalina Margulis and Arthur Rossi, “Legally Speaking, is Digital Money Really Money?”, IMF Blog, January 14, 2021. See also IMF Working Paper 2020/254 previously quoted in this report.

⁶² Id.

⁶³ At first glance, China seems to be leading the CBDC race. The Asian country launched domestic trials in Shenzhen, Chengdu and Hangzhou, and began research on CBDC back in 2014. In addition, China recently formed a joint venture with SWIFT, the global system for financial messaging and cross-border payments, signaling its intention to take the digital yuan global. For more details, see:

<https://www.reuters.com/article/china-swift-pboc/swift-sets-up-jv-with-chinas-central-bank-idU5L1N2KA0AK> (last accessed March 13, 2021). For a more comprehensive review of the digital yuan project, see Yaya J. Fanusie and Emily Jin, “China’s Digital Currency – Adding Financial Data to Digital Authoritarianism”, Center for New American Security, January 2021. Available at:

key foundational principles and preconditions to issue CBDC, which are discussed briefly in this report.⁶⁴ Quoting Jerome Powell, chairman of the US Federal Reserve System “...we have a responsibility to get this right – we don’t need to be the first.”⁶⁵ Below, we discuss recent CBDC developments in the EU and the US.

2. CBDC developments in the EU

a. Overview

On October 2, 2020 the European Central Bank (“ECB”) released a comprehensive report on the potential issuance of a digital euro (“DER”).⁶⁶ The DER was prepared by

<https://www.cnas.org/publications/reports/chinas-digital-currency> (last accessed March 13, 2021).

⁶⁴ BIS, “Central bank digital currencies: foundational principles and core features”, October 9, 2020, p. 10. Available at:

<https://www.bis.org/publ/othp33.htm> (last accessed March 8, 2021). This report was co-authored by the European Central Bank, the Board of Governors of the Federal Reserve System, the Bank of England, the BIS, and other central bank authorities. As a result, it arguably reflects a common, Transatlantic view on these topics.

⁶⁵ Jerome Powell’s testimony delivered to the US Senate Committee on Banking, Housing, and Urban Affairs on February 23, 2021. The full hearing can be accessed here: <https://www.banking.senate.gov/hearings/02/12/2021/the-semiannual-monetary-policy-report-to-the-congress> (last accessed February 28, 2021). Powell’s comments about the US digital dollar begin approximately at “1:39:50” of the recording.

⁶⁶ ECB, “Report on a digital euro”, October 2020. Available at:

the Eurosystem⁶⁷ High-Level Task Force on CBDC⁶⁸, and approved by the ECB Governing Council.⁶⁹ On October 12, 2020, the ECB launched a public consultation on the DER, which closed on January 12, 2021, yielding a record-high response from citizens, firms, and industry associations.⁷⁰

The public feedback highlighted privacy, security, and pan-European reach as top priorities for a digital euro.⁷¹ A comprehensive report summarizing the results of this consultation is expected to be released during

https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf (last accessed February 27, 2021).

⁶⁷ The DER analyzes the issuance of the digital euro, a CBDC, solely from the perspective of the Eurosystem. For reference, the Eurosystem comprises the ECB, a supranational institution with legal personality under international public law, and the National Central Banks of EU countries that have adopted the euro. Currently, there are 19 countries that have adopted the euro – this, in turn, is known as the euro area. The Eurosystem, and the so-called European System of Central Banks (ESCB), comprising also National Central Banks of countries that have not yet adopted the euro, will co-exist as long as there are EU countries outside the euro area. For more details on the Eurosystem, ECB, and ESCB please see:

<https://www.ecb.europa.eu/ecb/orga/escb/html/index.en.html> (last accessed February 28, 2021).

⁶⁸ In January 2020, the ECB Governing Council established this High-Level Task Force to advance the work around CBDC in the euro area. See ECB, “Report on a digital euro”, October 2020, p. 6. Available at: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf (last accessed February 27, 2021).

⁶⁹ See ECB, “ECB intensifies its work on a digital euro (press release)”, October 2, 2020. Available at: <https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr201002>

the northern-hemisphere spring of 2021.⁷² This report will be used by the ECB’s Governing Council to further explore whether and how to launch a digital euro project.⁷³ Below, we discuss the DER in greater detail.

b. The DER

According to this report, the digital euro would be a central bank liability offered in digital form for use by citizens and businesses for their *retail* payments.⁷⁴ It would complement, rather than substitute, the

[~f90bfc94a8.en.html](https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210113~ec9929f446.en.html) (last accessed February 27, 2021). The ECB Governing Council is the main decision-making body of the ECB. It consists of the six members of the Executive Board (i.e., president, vice-president, and four other members, all of which are appointed by the European Council through a qualified majority), plus the governors of the national central banks of the nineteen euro-area countries. For more details on the ECB Governing Council, please see: <https://www.ecb.europa.eu/ecb/orga/decisions/govc/html/index.en.html> (last accessed February 28, 2021). For more details on the ECB Executive Board, please see <https://www.ecb.europa.eu/ecb/orga/decisions/govc/html/index.en.html> (last accessed February 28, 2021).

⁷⁰ ECB, “ECB digital euro consultation ends with record level of public feedback (press release)”, January 13, 2021. Available at: <https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210113~ec9929f446.en.html> (last accessed February 27, 2021).

⁷¹ Id.

⁷² Id. Based on informal consultations with press officers at the ECB, this comprehensive report is expected to be released by mid-April 2021.

⁷³ Id.

⁷⁴ ECB, “Report on a digital euro”, October 2020, p. 3. Available at:

current offering of cash and wholesale central bank deposits in a secure way.⁷⁵

The digital euro would be designed to leverage efforts and developments made by other market participants, in the area of commercial banking and payment systems⁷⁶, thus fostering healthy competition and innovation. If issued, the digital euro would have to meet a series of requirements, such as:

(i) enhanced digital efficiency, to keep up with technology developments, while ensuring convenience and interoperability with other systems.⁷⁷

(ii) cash-like features, to allow offline payments and facilitate widespread, easy access, particularly by vulnerable groups.⁷⁸

(iii) competitive features, providing functionalities that are at least as attractive as those of other regulated or unregulated payment solutions.⁷⁹

(iv) monetary policy option, allowing the digital euro to bear interest, if needed, at rates controlled by the ECB.⁸⁰

(v) back-up system and cyber resilience, to ensure the overall monetary system can withstand potentially extreme events.⁸¹

https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf
(last accessed February 27, 2021).

⁷⁵ Id., p. 3.

⁷⁶ Id., p. 20.

⁷⁷ Id., p. 11.

⁷⁸ Id., p. 11.

⁷⁹ Id., pp. 12, and 21.

(vi) international use, to be accessible outside the euro area.⁸²

(vii) cost saving, to reduce costs in the current payment ecosystem.⁸³

(viii) environmentally friendly, to minimize its ecological footprint.⁸⁴

(ix) cooperation with market participants, including supervised and unsupervised intermediaries⁸⁵ (e.g., commercial banks and other payment systems providers).

(x) compliance with regulatory framework, even if ECB liabilities (like the digital euro) are not strictly subject to regulation and oversight.⁸⁶

By design, the digital euro should also comply with relevant legal frameworks. Below, we expand on select EU monetary law and central bank law issues.

c. Select legal aspects of the digital euro

From a legal perspective, the design of the digital euro will ultimately determine the legal basis for its issuance. Current EU law

⁸⁰ Id., p. 14.

⁸¹ Id., pp. 14, and 23.

⁸² Id., pp. 14, and 22.

⁸³ Id., pp. 15, and 21.

⁸⁴ Id., p. 15.

⁸⁵ Id., p. 20.

⁸⁶ Id., p. 20.

(primary and secondary)⁸⁷ does not expressly regulate issues pertaining to a digital form of the euro. However, according to the DER, such body of law would not preclude the Eurosystem from issuing a digital euro, be it in a wholesale or retail form, if needed.⁸⁸

If the digital euro were issued in a *wholesale form* (i.e., only accessible by commercial banks, like central bank reserves), the Eurosystem could invoke two legal provisions as legal basis. The first one would be article 127(2) of Treaty on the Functioning of the European Union (“TFEU”)⁸⁹, which *inter alia* empowers the European System of Central Banks (“ESCB”)⁹⁰ to define and implement the monetary policy of the EU. The second provision would be article 20 of the Statute of the ESCB and the ECB⁹¹, which authorizes the ECB Governing Council to leverage “*other operational methods of monetary control*” to comply with the ESCB’s primary objective of maintaining price stability, and

to support general economic policies in the EU.

If the digital euro were issued in a *retail form* (i.e., widely accessible by the public, like cash) and became available to households and other private entities through accounts held with the Eurosystem (i.e., a retail, account-based digital euro), the Eurosystem could also invoke two provisions. The first one would be article 127(2) of the TFEU, which we already explained. The second one would be article 17 of the Statute of the ESCB and the ECB, which authorizes the ECB, and the National Central Banks in the euro area, to open accounts for credit institutions and other market participants.

The DER does not appear to explicitly address the legal basis for issuing a retail, token-based digital euro. It does mention, however, that if the digital euro were issued “*as an instrument equivalent to a banknote*”⁹² the Eurosystem could invoke, as the

⁸⁷ Treaties are known as EU primary law. The body of law that emanates from principles and objectives of those treaties is known as EU secondary law, and includes regulations, directives, decisions, recommendations, and opinions. See “Types of EU Law” at https://ec.europa.eu/info/law/law-making-process/types-eu-law_en (last accessed February 27, 2021).

⁸⁸ ECB, “Report on a digital euro”, October 2020, p. 24. Available at: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf (last accessed February 27, 2021).

⁸⁹ Id. p. 24.

⁹⁰ See footnote 67 for more details on the relationship between ESCB, ECB, and the Eurosystem.

⁹¹ ECB, “Report on a digital euro”, October 2020, p. 24. Available at:

https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf (last accessed February 27, 2021).

⁹² As discussed, banknotes are considered physical tokens carrying a promise to pay to their holders. Banknotes are widely accessible by the public (akin a retail form of CBDC). Having this in mind, can the categorization of the digital euro as an “*instrument equivalent to a banknote*” be reasonably construed as referring to a *retail, token-based digital euro* and, thus, that this form of digital euro can be legally issued under the current legal framework? For context, there is a growing debate in the legal community as to whether central banks have the legal authority to issue token-based CBDC (as opposed to account-based CBDC), under their current legal frameworks, or whether reform is needed. According to the previously

most expedient legal basis for its issuance, two provisions. The first one would be article 128 of the TFEU⁹³, which grants the ECB the “*exclusive right to authorize the issuance of euro banknotes*” within the EU. The second provision would be the first sentence of Article 16 of the Statute of the ESCB and the ECB⁹⁴, which grants this exclusive right specifically to the ECB Governing Council, while stating that the ECB and National Central Banks within the euro area may issue euro banknotes, and that such notes are the *only* notes that have legal tender status within the euro area.⁹⁵

Albeit this last provision appears to narrow the application of legal tender status *only* to euro banknotes⁹⁶, neither the TFEU nor the Statute of the ESCB and the ECB, would

expressly prevent the Eurosystem from issuing other forms of liabilities.⁹⁷ In fact, the DER suggests that the “*right to issue ‘euro banknotes’ could be understood to encompass the right to determine the format or medium of ‘euro banknotes’*”.⁹⁸ As a result, the DER concludes that the digital euro, if treated as euro banknotes, could have legal tender status under current legislation.⁹⁹

In short, based on the DER, it appears that the Eurosystem would be legitimized to issue a retail or wholesale form of digital euro, either account-based or token-based, under its current central bank and monetary legal frameworks, without the need for extensive reform.

quoted IMF working paper on legal aspects of CBDC, for a central bank to be able to legally issue token-based CBDC, its legal framework most likely would need to include (i) an explicit *function* for that central bank “*to issue currency*” in general, without limiting the issuance of currency only to banknotes and coins; and (ii), the associated “*powers*”, if needed under local law, to implement this function, making explicit reference, in this case, to the issuance of currency in the form of banknotes, coins, and digital tokens. For more details on this discussion, please see Wouter Bossu; Masaru Itatani; Catalina Margulis; Arthur D. P. Rossi; Hans Weenink; Akihiro Yoshinaga, “Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations”, Working Paper No. 2020/254, p. 11 (general discussion on token-based CBDC) and p. 26, paragraph 50 (central bank law reform recommendations around token-based CBDC). Available at: <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827> (last accessed February 28, 2021).

⁹³ ECB, “Report on a digital euro”, October 2020, p. 24. Available at: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf (last accessed February 27, 2021).

⁹⁴ Id., p. 24.

⁹⁵ Id., p. 24.

⁹⁶ As discussed in footnote 40, Articles 10 and 11 of the Council Resolution (EC) No. 974/98, extend legal tender status to euro coins, as well.

⁹⁷ Id., p. 25.

⁹⁸ Id., p. 25. Based on this specific statement, it appears that the Eurosystem could, in fact, determine the format of issuance of the digital euro. As a result, it could be construed that the Eurosystem could potentially issue a retail, token-based digital euro (i.e., this would be a different format compared to a retail, account-based digital euro). If this were true, it could be further construed that a retail, token-based digital euro might be able to enjoy legal tender status in the EU, under the previously referred legal framework.

⁹⁹ Id., p. 25.

3. CBDC developments in the US

a. Overview

On August 13, 2020, the Board of Governors of the Federal Reserve System (“Fed”)¹⁰⁰ issued a press release highlighting that, given the importance of the US

¹⁰⁰There is no single central bank institution in the US. Rather, there is a central banking system, the Fed, which is comprised by three types of entities: **(i)** the Board of Governors; **(ii)** twelve Reserve Banks and their branches; **(iii)** and the Federal Open Market Committee (“FOMC”).

The Board of Governors, a federal agency that reports directly to Congress, is the governing body of the Fed, which oversees the operations of 12 decentralized Reserve Banks, and shares responsibility with them in the supervision and regulation of certain financial institutions and activities.

Reserve Banks, in turn, are distributed across 12 districts, which reflect certain trade regions that existed back in 1913, when the Fed was created. Reserve Banks, and their 24 branches, are the operating arms of the Fed. Most Reserve Banks have at least one branch. Among other functions, Reserve Banks typically **(i)** supervise state members banks (i.e., state-chartered banks that agreed to become part of the Fed); **(ii)** lend to depository institutions; **(iii)** oversee certain financial institutions and activities; and **(iv)** provide key financial services, including distributing US currency (i.e., banknotes) and coins to depository institutions, while serving as a bank for the US Treasury and district-level commercial banks, thrifts, and credit unions. Each Reserve Bank gathers key monetary and economic data about its district, which is subsequently shared with the FOMC.

The FOMC, in turn, leverages the data gathered by Federal Reserve Banks, and other information, to set the national monetary policy, which is its primary function, and to make all

dollar for the national and international economy, it is essential for the Fed to remain on the frontier of research and policy development in the area of CBDC.¹⁰¹

On the same day, the Federal Reserve Bank of Boston launched a multi-year collaboration with the Massachusetts Institute of Technology (“MIT”)¹⁰² to explore the use of existing and new technologies to build

decisions around the conduct of open market operations. Open market operations refer to the purchase and sale of US Treasury bonds or other securities in the market.

Finally, the Fed, on aggregate, performs five core functions to support the effective operation of the US economy. Those functions are: **(i)** conducting monetary policy; **(ii)** promoting financial system stability; **(iii)** supervising and regulating financial institutions and activities; **(iv)** fostering payment and settlement system safety and efficiency; and **(v)** promoting consumer protection and development.

For a more detailed review of the Fed’s structure, its functions, and institutions, please see Board of Governors of the Federal Reserve System, “The Federal Reserve System – Purposes and Functions”, 10th Edition (2016), Washington D.C., Chapters 1 and 2. Available at: https://www.federalreserve.gov/aboutthefed/files/pf_complete.pdf (last accessed February 28, 2021).

¹⁰¹ Board of Governors of the Federal Reserve System, “Federal Reserve highlights research and experimentation undertaken to enhance its understanding of the opportunities and risks associated with central bank digital currencies”, Press Release, August 13, 2020. Available at: <https://www.federalreserve.gov/newsevents/pressreleases/other20200813a.htm> (last accessed March 2, 2021).

¹⁰² More specifically, the collaboration is with MIT’s Digital Currency Initiative. To learn more about this initiative, please visit: <https://dci.mit.edu/> (last accessed March 2, 2021).

and test “a hypothetical digital currency platform.”¹⁰³ Ever since, staff of these two institutions have participated in several virtual events, sharing their thoughts on CBDC technology-related matters, such as interoperability standards, privacy-preserving techniques, and cybersecurity.¹⁰⁴

On February 23, 2021, Jerome Powell appeared before the US Senate Committee on Banking, Housing, and Urban Affairs to deliver the first part of the Semiannual Monetary Policy Report to Congress.¹⁰⁵ During his testimony, Powell mentioned that “[they] are looking carefully, very carefully at the question of whether [the US] should issue a digital dollar”¹⁰⁶, while underscoring the Fed’s commitment “to consulting very broadly with the public and very transparently with all interested constituencies”¹⁰⁷.

The digital dollar seems to be a “very high priority project”¹⁰⁸ for the Fed.

In addition to the digital dollar initiative, the Fed has been actively exploring the development of an instant-payment service system called FedNow.¹⁰⁹ FedNow would allow financial institutions of every size, across any community in the US, to provide safe and efficient payment services in real time, 24 hours a day, every day of the year.¹¹⁰ It is unclear at this stage how a digital dollar, if issued, would interact with FedNow.

Shortly after Powell’s appearance before Congress, a paper outlining the pre-conditions for issuing a general-purpose central bank digital currency (i.e., a retail digital dollar) was released through the so-called “FEDS Notes”¹¹¹, a Fed’s publication. This

¹⁰³ Federal Reserve Bank of Boston, “The Federal Reserve Bank of Boston announces collaboration with MIT to research digital currency”, Press Release, August 13, 2020. Available at: <https://www.bostonfed.org/news-and-events/press-releases/2020/the-federal-reserve-bank-of-boston-announces-collaboration-with-mit-to-research-digital-currency.aspx> (last accessed March 2, 2021).

¹⁰⁴ See, for example, recently hosted virtual event on “Technology Behind CBDC and The Retail Use Case”. Available at: <https://www.eventbrite.com/e/technology-behind-central-bank-digital-currencies-and-the-retail-use-case-tickets-139268338349#> (last accessed March 2, 2021).

¹⁰⁵ The full committee hearing can be accessed here: <https://www.banking.senate.gov/hearings/02/12/2021/the-semiannual-monetary-policy-report-to-the-congress> (last accessed February 28, 2021).

¹⁰⁶ Id., starting at 1:39:50.

¹⁰⁷ Id., starting at 1:40:27.

¹⁰⁸ Id., starting at 1:41:30.

¹⁰⁹ See press release issued on August 6, 2020 by the Fed’s Board of Governors with more details on the FedNow initiative here:

<https://www.federalreserve.gov/newsevents/pressreleases/other20200806a.htm> (last accessed March 14, 2021).

¹¹⁰ See “About the FedNow Service” here: <https://www.frbservices.org/financial-services/fednow/about.html> (last accessed March 14, 2021).

¹¹¹ Cheng, Jess, Angela N Lawson, and Paul Wong (2021). “Preconditions for a general-purpose central bank digital currency,” FEDS Notes. Washington: Board of Governors of the Federal Reserve System, February 24, 2021. Available at: <https://doi.org/10.17016/2380-7172.2839> (last accessed February 28, 2021). This paper does not deal with a wholesale form of digital dollar.

paper is further discussed in the next section.

b. The FEDS Note on preconditions for issuing a general purpose CBDC

The FEDS note groups these preconditions into five areas, namely: **(i)** clear policy objectives; **(ii)** broad stakeholder support; **(iii)** robust technology; **(iv)** market readiness; and **(v)** strong legal framework.¹¹²

Clear policy objectives

The design of CBDC should be guided by clear policy objectives, and not the other way around. Therefore, a digital dollar should be consistent with the Fed's core functions, which *inter alia* include maintaining the safety and efficiency of the nation's payments system and ensuring monetary and financial stability.¹¹³

A digital dollar also needs to adhere to three key principles, outlined in a report produced by the BIS, the Fed, the ECB, and other central bank authorities.¹¹⁴ Those principles are: **(i)** "do not harm" monetary and financial stability; **(ii)** complement existing forms of

money; **(iii)** and support innovation and efficiency.¹¹⁵

Broad stakeholder support

Consistent with Powell's comments above, the FEDS note specifically highlights the need to engage with, and mobilize, a broad base of stakeholders to ensure a digital dollar has ample support across sectors, and geographies. Relevant stakeholders to be consulted include:

(i) governments, to navigate legal and regulatory implications of issuing CBDC, both at the domestic and international levels, while helping drive societal change.¹¹⁶

(ii) end users, to ensure that the digital dollar is specifically designed to address the needs of individuals, businesses, and community organizations.¹¹⁷

(iii) financial institutions¹¹⁸, because introducing CBDC, specially in a retail form, can have implications for their role in the monetary system.

¹¹² Id.

¹¹³ Id. Also, see footnote 100 for more details on these and other functions performed by the Fed.

¹¹⁴ Id.

¹¹⁵ Id. See also BIS, "Central bank digital currencies: foundational principles and core features", October 9, 2020, p. 10. Available at: <https://www.bis.org/publ/othp33.htm> (last accessed March 8, 2021).

¹¹⁶ Cheng, Jess, Angela N Lawson, and Paul Wong (2021). "Preconditions for a general-purpose central bank digital currency," FEDS Notes. Washington: Board of Governors of the Federal Reserve System, February 24, 2021. Available at: <https://doi.org/10.17016/2380-7172.2839> (last accessed February 28, 2021).

¹¹⁷ Id.

¹¹⁸ Id.

(iv) technology and infrastructure providers, to ensure fit-for-purpose technological innovations are always leveraged.¹¹⁹

(v) academia and think tanks, to provide thought leadership to inform policymaking.¹²⁰

(vi) standard setting organizations, to define terms, taxonomies, specifications and standards, in support of the broader CBDC ecosystem.¹²¹

Robust technology

Issuing a retail digital dollar will also require extensive technology assessment and development work, across three key areas:

(i) system integrity, so that the digital dollar is able to operate in an unimpaired fashion, while being free from unauthorized manipulation. Thus, the system should enable a secure and efficient transfer of assets; allow accurate recordkeeping with robust fraud detection capabilities; and possess strong information security controls.¹²²

(ii) operational robustness, so that the digital dollar functions correctly and reliably across a range of operational scenarios. As a result, the system should be available 24 hours a day, every day of the year; it must leverage flexible and adaptable technology

to respond to future needs; and factor in the robustness of the ecosystem as a whole, and not just that of a specific actor in the ecosystem.¹²³

(iii) operational resilience, so that CBDC can resist, absorb, recover from, or adapt to, adverse events. Consequently, the system should have end-to-end resilience (i.e., measured at the end user level, and not just at the interbank settlement function level). It should also be resilient from a people, information, processes, and facilities perspectives, while factoring in potential disruptions caused by connectivity outages.¹²⁴

Market readiness

Whether the market is ready for the digital dollar is largely a function of *evident demand* and *evident supply*. Evident demand refers to the general population's willingness to accept the digital dollar as a payment instrument, amidst a wide range of other payment options.¹²⁵ Evident supply refers to the readiness of the digital dollar ecosystem as a whole (not just of the Fed) to properly support the issuance, distribution, storage, and usage of CBDC.¹²⁶

There are driving and restraining forces in favor and against, respectively, of CBDC adoption. Among the driving forces, we find the desire for innovation, advances in

¹¹⁹ Cheng, Jess, Angela N Lawson, and Paul Wong (2021). "Preconditions for a general-purpose central bank digital currency," FEDS Notes. Washington: Board of Governors of the Federal Reserve System, February 24, 2021. Available at: <https://doi.org/10.17016/2380-7172.2839> (last accessed February 28, 2021).

¹²⁰ Id.

¹²¹ Id.

¹²² Id.

¹²³ Id.

¹²⁴ Id.

¹²⁵ Id.

¹²⁶ Id.

technological capabilities, and solving key problems faced by interested parties in the monetary ecosystem.¹²⁷ Among the restraining forces, we find wide acceptance of other forms of payment (including cash), immature technologies, and significant coordination challenges.¹²⁸

Strong legal framework

The FEDS note underscores the need for a strong legal framework supporting the issuance of a digital dollar. Below, we discuss select legal issues under US central bank and monetary law.

c. Select legal aspects of the digital dollar

¹²⁷ Id.

¹²⁸ Id.

¹²⁹ Under section 16(1) of the FRA, the Fed's Board of Governors is empowered to issue so-called Federal Reserve Notes. Those notes are redeemable by lawful money at the US Treasury. While the Fed issues federal reserve notes, the US Treasury, through its Bureau of Engraving and Printing, engraves and prints them. The US treasury, through its US Mint Bureau, also mints coins. Coins and currency (i.e., notes), as discussed before, have legal tender status in the US under section 5103 of the US Code and, thus, are lawful money. According to section 16(2) of the FRA, Federal Reserve Banks can apply to access Federal Reserve Notes, provided they issue collateral in an equivalent amount. Collateral is not required, however, if Federal Reserve Notes are held in the vaults, or are otherwise held by, or on behalf of, Federal Reserve Banks. It is easy to visualize the potentially disruptive effects that a retail digital dollar can have in this system. If a retail digital dollar were issued directly by the Fed to the public: **(i)** how would the US Treasury's role change, considering a digital dollar would not need to be engraved, printed,

The Fed exercises the powers and functions specifically authorized by the Federal Reserve Act ("FRA"). Under the FRA, the Fed's Board of Governors is empowered to issue Federal Reserve Notes (i.e., banknotes), and to provide payment services to depository institutions and other entities.¹²⁹ In this context, the FEDS note poses the question of whether amendments to the FRA are needed to explicitly allow the Fed to issue a retail digital dollar. Compared to the DER, the FEDS note seems to follow a more conservative approach, suggesting the need for further analysis to specifically conclude on whether the Fed has the legal authority to issue CBDC.

or minted in the traditional sense of these terms? **(ii)** what would the role of commercial banks be, if, for example, they no longer had to intermediate between the Fed, the Federal Reserve Banks, and the general public? **(iii)** what would the role of the Fed's Board of Governors be, compared to that of Federal Reserve Banks? For more details on the US central bank system, please refer to footnote 100. For more details on how money is created in the US, please visit the following links: **(i)** open market operations - <https://www.federalreserve.gov/monetarypolicy/openmarket.htm> (last accessed March 11, 2021); **(ii)** discount rate - <https://www.federalreserve.gov/monetarypolicy/discountrate.htm> (last accessed March 11, 2021); **(iii)** reserve requirements - <https://www.federalreserve.gov/monetarypolicy/reservereq.htm> (last accessed March 11, 2021); **(iv)** FRA, section 16 governing the issuance of Federal Reserve Notes - <https://www.federalreserve.gov/aboutthefed/section16.htm> (last accessed March 11, 2021); **(v)** US treasury role in the creation of money - <https://home.treasury.gov/services/currency-and-coins> (last accessed March 12, 2021).

Under current monetary law, in turn, only coins and currency (i.e., banknotes) have legal tender status in the US with respect to debts, public charges, taxes, and dues.¹³⁰ It is therefore unclear whether legal tender status would automatically extend to the digital dollar, or whether section 5103 of the US code would need to be amended to explicitly grant legal tender status to CBDC.

As discussed before, even if the digital dollar had legal tender status, this would not necessarily guarantee its wide acceptance by the public. Widespread acceptance will ultimately depend on the credibility and convenience of the digital dollar compared to other means of payment, including cash and bank deposits.

4. Key takeaways

The field of CBDC is still in its infancy around the world, albeit jurisdictions like

China seem to be leading the pack. The EU and US are both at an early research stage. Given the implications that a digital euro or digital dollar can have for the global monetary system and economy, policymakers are approaching this matter carefully, while consulting extensively with a broad group of stakeholders.

Beyond the monetary law and central bank law issues briefly discussed in this report, the issuance of CBDC will have implications across other areas of law, as well. Those include, for example: **(i)** tax law¹³¹; **(ii)** privacy and data protection law¹³²; **(iii)** anti-money laundering, countering the financing of terrorism, and know your client (AML/CFT/KYC) law¹³³, to mention a few.

For the most part, if CBDC are issued, their adoption will pose interesting behavioral science questions. Governments around the world are leveraging behavioral insights to design and implement public policy more effectively.¹³⁴ These behavioral insights

¹³⁰ Section 5103 of the US Code.

¹³¹ For tax purposes, one of the key issues is whether countries will treat CBDC as “property”, as most of them have done with respect to non-central bank digital currencies, or whether they will treat CBDC as “currency”. The tax implications of each categorization tend to be very different. Another interesting topic in the tax arena relates to the ability to “program” CBDC to facilitate, for example, the automatic payment of so-called withholding taxes at source, and ultimately help reduce the risk of tax fraud in cross-border operations.

¹³² CBDC may impact privacy, for example, by making the transfer of funds easier to trace. Therefore, the design of CBDC should be consistent with applicable data privacy and data protection laws to avoid a surveillance state.

There are several privacy-preserving techniques currently being explored. See, for example, Bank of Canada, “Privacy in CBDC Technology”, Note 2020-9, June 2020. Available at: <https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-9/> (last accessed March 15, 2021).

¹³³ In case a retail form of CBDC is issued, a key question is whether central banks will assume some of the AML/CFT/KYC functions normally performed by commercial banks vis-à-vis their clients.

¹³⁴ Cass R. Sunstein, “Behavioral Science and Public Policy”, Cambridge University Press, 2020. See, in particular, pp. 26 and 27 highlighting behavioral insights in the area of banking and finance.

could be used to design CBDC that are convenient, practical, and add value to relevant users. As professor Ronald Heifetz puts it: “*people do not resist change, per se; people resist loss.*”¹³⁵ Thus, understanding what users might lose if CBDC are implemented will be key to overcome resistance and ultimately drive adoption.¹³⁶

¹³⁵ Ronald Heifetz, in Richard A. Couto, ed., “Political and Civil Leadership: A Reference Handbook”, SAGE Publications, 2010, p. 17.

¹³⁶ Heifetz states that “*when people know that change will be good for them, they embrace*

change... People resist change when the change is likely to involve loss. Change can involve loss of various kinds: direct losses of status, wealth, security, or loved ones; loss of competency; or loss of loyalty.” Id., p. 17.

Other Developments

European Union

Democratic Countries Should Form a Strategic Tech Alliance

By Mauritz Kop¹³⁷

1. Introduction

In December 2020, Europe reached a comprehensive multi-billion-dollar investment agreement (CAI) with China.¹³⁸ As the United States (US) are facing the challenges of intensified competition with China, the deal has come under some criticism by

the Biden Presidency.¹³⁹ The question arises whether differing US and EU strategies towards China are damaging transatlantic relations¹⁴⁰, and whether the world would be better off with a united US-EU front.¹⁴¹

China's relentless advance in Artificial Intelligence (AI) and quantum computing has engendered a significant amount of anxiety about the future of America's technological supremacy.¹⁴² Currently, China is leading in quantum technology, the US still have a slight edge in AI.¹⁴³ The resulting debate centres around the impact of China's digital rise on the economy, security, employment and the profitability of American companies. Absent in these predominantly economic disquiets is what should be a deeper, existential concern: What are the effects of authoritarian regimes¹⁴⁴ exporting their values into our society through their technology?¹⁴⁵ This essay will address this question by

¹³⁷ [Mauritz Kop](#) is a Stanford Law School TTLF Fellow and Managing Partner at [AlRecht](#), a leading 4th Industrial Revolution technology consultancy firm based in Amsterdam, The Netherlands. The author is grateful to Suzan Slijpen (Slijpen [Legal](#)) for valuable comments on an earlier version of this article, and to Juha Vesala and his team for excellent editorial support.

¹³⁸ See: <https://edition.cnn.com/2020/12/31/asia/eu-china-trade-deal-human-rights-us-intl-hnk/index.html>

¹³⁹ See: <https://www.nytimes.com/2020/12/23/business/china-european-union-united-states.html>

¹⁴⁰ See: <https://www.politico.eu/article/why-europe-china-investment-deal-will-poison-transatlantic-relations-joe-biden/>

¹⁴¹ See also: <https://www.atlantic-council.org/event/transatlantic-cooperation-in-the-era-of-ai/>

¹⁴² See: <https://edition.cnn.com/2020/11/15/asia/biden-china-policy-trump-us-intl-hnk/index.html>

¹⁴³ See for example: <https://hai.stanford.edu/research/ai-index-2021> and <https://www.newsweek.com/2020/12/25/china-leads-quantum-computing-race-us-spies-plan-world-fewer-secrets-1554439.html>

¹⁴⁴ See for a list of authoritarian regimes: <https://www.wearethemighty.com/lists/the-21-most-authoritarian-regimes-in-the-world/>

¹⁴⁵ See also: Roundtable: A 'China Model?' Beijing's Promotion of Alternative Global Norms and Standards, U.S.-China Economic AND Security Review Commission, April 27, 2020, <https://www.uscc.gov/hearings/roundtable-china-model-beijings-promotion-alternative-global-norms-and-standards>

examining how democratic countries can, or should respond, and what you can do about it to influence the outcome.

The essay argues that democratic countries should form a global, broadly scoped Strategic Tech Alliance, built on mutual economic interests and common moral, social and legal norms, technological interoperability standards, legal principles and constitutional values.¹⁴⁶ The US, the EU and its democratic allies should join forces with countries that share our digital DNA, institute fair reciprocal trading conditions, and establish a global technology governance framework that actively pursues democratic freedoms, human rights and the rule of law.¹⁴⁷ In this essay, ‘democratic norms’ refer to the principles and values as enshrined in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). The essay concludes that to prevent authoritarianism from gaining ground, governments should do three things: (1) inaugurate a Strategic Tech Alliance, (2) set worldwide core rules, interoperability & conformity standards for key 4IR (Fourth Industrial Revolution) technologies such as AI,

¹⁴⁶ See also: <https://beyondstandards.ieee.org/ieee-7010-2020-launch-prioritizes-human-well-being-and-environmental-sustainability-via-technology/>

¹⁴⁷ See also: <https://www.scmp.com/comment/opinion/article/3118137/china-eu-investment-deal-shows-biden-united-front-trade-will-not-be>

¹⁴⁸ See: Mauritz Kop, Machine learning and EU data-sharing practices: Legal aspects of machine learning training datasets for AI systems, (March 3, 2020). Research Handbook on Big Data Law

quantum, 6G and Virtual Reality (VR), and (3) actively embed our common democratic norms, principles and values into the architecture and infrastructure of our technology.¹⁴⁸

2. The Challenge

Technology is shaping our everyday lives. The way in which we design and use our technology is influencing nearly every aspect of the society we live in.¹⁴⁹ The opposite is also true: the type of society we live in, its norms and standards, shapes the architecture of technology. Technology is never neutral: our society’s norms and values are reflected in the technology we produce. As society shapes technology, technology shapes society.

For example, privacy preserving techniques used in machine learning algorithms help to safeguard privacy: a fundamental, constitutional freedom. Protecting privacy features high on the list of priorities in a society that cherishes human rights.¹⁵⁰ On the other end of the spectrum are facial and voice

edited by Roland Vogl, Chapter 22, pp. 431-452, Edward Elgar Publishing Ltd., 2021, Forthcoming.

¹⁴⁹ See also: Ünver, H. Akin. *Artificial Intelligence, Authoritarianism and the Future of Political Systems*. Centre for Economics and Foreign Policy Studies, 2018, www.jstor.org/stable/resrep26084.

¹⁵⁰ See for example: <https://plato.stanford.edu/entries/it-privacy/> and <https://www.technologyreview.com/2018/12/14/138615/its-time-for-a-bill-of-data-rights/>

recognition techniques used for a social crediting system. These have no place in a democracy.

Just like we embed our own values in our hi-tech systems, the authoritarian regimes do the same. With authoritarianism I mean autocratic governments that have a culture with less political participation, less checks and balances and less civil liberties.¹⁵¹ Societies with social norms, democratic standards and ethical priorities that are incompatible with our own system.

Subsequently, the regimes export their undemocratic ideology to our society through the construction, dissemination and functionality of their technology.¹⁵² Main contributors to this spread of culture and ideology through technology are the Belt & Road Initiative, Confucius Institutes and Chinese multinationals.¹⁵³ I am referring here to central 4IR technologies such as 5G infrastructures, AI, big data and quantum computing.¹⁵⁴ Excesses involve automated social profiling systems that monitor and hinder online dissidence. This process of exporting an incompatible political ideology through technology holds the danger of permanently weakening the health of our democracy, including the rights and freedoms we care so deeply about. We should prevent that from happening.

¹⁵¹ Such as the Chinese Communist Party and the Kremlin.

¹⁵² See also: <https://www.washingtonpost.com/technology/2020/11/16/biden-huawei-trump-china/>

¹⁵³ See also: The National Endowment for Democracy, Sharp Power and Democratic

It is important to note that we do not intend to exclude the people who are living in authoritarian or even totalitarian regimes such as China, Russia, Iran and North Korea, nor the companies that are willing to abide to democratic technological standards. Instead, our strategy should be to avoid the ideas of the regimes that are incorporated in their technology, which is never neutral.

3. The Response

What needs to be done and who should do it?

Democratic Countries Should Form a Strategic Tech Alliance. That's the first, foundational step.

The US and its democratic allies should establish a strong, broadly scoped Strategic Tech Alliance with countries that share our digital DNA. An Alliance built on strategic autonomy, mutual economic interests and shared democratic & constitutional values. Main purpose of the Strategic Tech Alliance is to win the race / stay ahead of the competition.

Multilateral cooperation with any country that has matched concerns about the outcome of the race for AI & quantum

Resilience Series, February 12, 2020, <https://www.ned.org/sharp-power-and-democratic-resilience-series/>.

¹⁵⁴ See also: <https://edition.cnn.com/2020/10/30/world/trump-china-xi-election-intl-hnk/index.html>

dominance in view of democratic values, is paramount. A natural starting point for a geopolitical dialogue on disruptive technology that is also in the focus of President Biden, is Transatlantic cooperation.¹⁵⁵ In addition to the US, EU, UK & Canada, countries such as India, Israel, Japan, South-Korea, Taiwan and Australia would be great candidates to join the cause. The Strategic Tech Alliance could also connect with existing structures such as NATO.

Moreover, it is crucial and urgent that democratic countries set worldwide technology standards together. This includes the development of globally accepted benchmarks and certification. Standards based on safety, security and interoperability, with respect for our common Humanist moral values.¹⁵⁶ Values in which the rule of law and human dignity play a leading part.

Consequently, AI & quantum products and services made within the territory of the Strategic Tech Alliance or elsewhere in the world, should adhere to specific safety and security benchmarks, before they qualify for market authorization. These should follow the high technical, legal and ethical

standards that reflect Responsible, Trustworthy AI & quantum technology core values. Ex ante certification comparable to the USA Compliance Marking or the European CE-marking should be mandatory before AI and quantum infused products and services are eligible to enter the Transatlantic markets.¹⁵⁷

In this vision, the Strategic Tech Alliance should regulate transformative technology in a harmonized way across member countries. Using a risk-based approach that incentivises sustainable innovation. For example, the Strategic Tech Alliance would share core horizontal rules that govern the production and distribution of transformative tech systems. Think of universal, overarching guiding principles of Trustworthy and Responsible AI & quantum technology that are in line with the distinctive physical characteristics of quantum mechanics.¹⁵⁸ Technology that gained the trust of the general public has significant marketing advantages.

To preserve pre-pandemic life as we knew it, we must bake our norms, standards, principles and values into the design of our

¹⁵⁵ See also: <https://www.politico.eu/article/long-term-significance-of-new-transatlantic-agenda/>

¹⁵⁶ Mauritz Kop, *Beyond AI & Intellectual Property: Regulating Disruptive Innovation in Europe and the United States – A Comparative Analysis*, <https://law.stanford.edu/projects/beyond-ai-intellectual-property-regulating-disruptive-innovation-in-europe-and-the-united-states-a-comparative-analysis/>

¹⁵⁷ Mauritz Kop, *Shaping the Law of AI: Transatlantic Perspectives*, TTLF Working Papers No. 65, Stanford-Vienna Transatlantic

Technology Law Forum (2020), <https://law.stanford.edu/publications/no-65-shaping-the-law-of-ai-transatlantic-perspectives/>. See also: https://ec.europa.eu/growth/single-market/ce-marking_en

¹⁵⁸ For a detailed description of ethical, legal and social guiding principles for quantum technology, see: Mauritz Kop, *Establishing a Legal-Ethical Framework for Quantum Technology*, (February 28, 2021), Yale Journal of Law & Technology (YJoLT) The Record 2021, Forthcoming

advanced hi-tech-systems.¹⁵⁹ From the first line of code. We can accomplish this by pursuing responsible, Trustworthy tech: by actually building socially & ethically aligned AI and quantum architectures and infrastructures.¹⁶⁰ We should incorporate our values *en bloc* and make our uniform design standards and (inter)operational requirements mandatory by law. A Strategic Tech Alliance could be the engine.

4. Political Feasibility

Let us discuss arguments against the formation of a democratic, value-based Strategic Tech Alliance that will set global technology standards. First, is establishing an Alliance that opposes the authoritarian tech agenda a realistic, politically feasible scenario or mere naive utopian thinking? Will the ambition of harmonized, global technology standards be limited by a cold shorter-term sum of costs and benefits? Will Realpolitik make it fade away in beauty?

Let's start with the United States. After the Democrats recently recaptured Senate majority, progressive policies might regain momentum. But still, forming an Alliance and setting joint tech governance goals would require a bipartisan, bicameral effort. It

would require large majorities to prevent legislative filibusters. Moreover, President Biden's primary policy objectives are battling COVID-19 together with relief measures, Medicare for All, rebuilding the country's infrastructure and fighting climate change. Regulating Big Tech and its impact on society might have less priority. However, winning the race for AI & quantum ascendancy should be high on any president's agenda.¹⁶¹

Then the EU. In recent years, the European Commission has been very active and progressive in the field of legal-ethical frameworks for emerging tech, including the conception of responsible AI and data governance models. Since it has become clear that MAGA (Make America Great Again) will no longer be the leading ideology in America for the next 4 years, Ursula von der Leyen's Team has not missed a single opportunity to strengthen transatlantic ties and inject political momentum into the relationship. With the main goal of implementing a mutual tech governance agenda, and jointly managing the geopolitics of exponential technology.

An exception to this rule was the recent EU-China deal, which raised quite a few eyebrows in Washington.¹⁶² This trade deal makes clear that economic interests of Western democratic countries in China, in

¹⁵⁹ See also: Kara Frederick, Democracy by Design - An Affirmative Response to the Illiberal Use of Technology for 2021, CNAS, December 15 2020, <https://www.cnas.org/publications/reports/democracy-by-design>

¹⁶⁰ See also: <https://www.aitrends.com/videos/artificial-intelligence-the-alpha-trend/>

¹⁶¹ See also: <https://www.technologyreview.com/2021/01/22/1016652/biden-administration-ai-plans-what-to-expect/>

¹⁶² See: <https://www.nytimes.com/2020/12/30/business/china-eu-investment-deal.html>

this case prompted by commercial interests of the German car industry and the Silk Road Initiative, may stand in the way of the targeted team effort needed to achieve the envisaged Strategic Tech Alliance.¹⁶³ As of 2020, the EU has surpassed the US as China's largest trading partner (numbers). The economic interests are gigantic and vary widely from one Member State to another.¹⁶⁴ For example, the Netherlands, a country of 17 million people, has an annual trade deficit with China of no less than 70 billion euros. Therefore, one might think that the EU will be less likely to 'turn away' from China and choose sides.

It is to be hoped that Europe has not been lulled into blissful sleep by the Chinese siren song of smart partnerships, better working conditions, respect for intellectual property and fair trade & investment opportunities.¹⁶⁵ The idea that the Chinese Party apparatus will allow more openness is a strategic misconception.¹⁶⁶ The opposite of openness, reliability, honesty and a fair level playing field happens every day before our eyes in Hong Kong.¹⁶⁷ And it doesn't get any better.

¹⁶³ See: <https://www.politico.eu/article/eu-china-investment-deal-angela-merkel-pushes-finish-line-despite-criticism/>

¹⁶⁴ See: <https://www.politico.eu/article/germans-drive-for-eu-china-deal-draws-criticism-from-other-eu-countries/>

¹⁶⁵ See also: <https://www.politico.eu/article/paris-will-block-eu-china-deal-says-trade-minister/>

¹⁶⁶ See also: <https://www.project-syndicate.org/commentary/eu-china-investment-agreement-criticisms-by-daniel-gros-2021-02>

¹⁶⁷ See also: <https://www.ny-times.com/2020/09/17/world/asia/china-europe-xi-jinping.html>

Entirely in line with the autocratic paradigms of systematic repression, inequality, arbitrariness, state surveillance and control.¹⁶⁸

It is not expected that the political situation and civil liberties & human rights in China will change in the short or medium term. We are competing with a political ideology that is fundamentally at odds with our own system.¹⁶⁹

In addition, internal divisions within the EU Member States may delay the rollout of progressive political initiatives.¹⁷⁰ Facing the portrayed challenges, Europe should speak with one voice. Further, it is to be hoped that European ambitions towards strategic autonomy and data sovereignty will not stand in the way of transatlantic partnerships in the field of AI and quantum computing, quantum sensing and the quantum internet.

Second, is there sufficient political will, enough common ground between the various continents and countries to forge such an Alliance, comparable to the foundation of the United Nations in 1945 after World War II? There currently seem to be diverging

¹⁶⁸ See also: Wright, Nicolas D., Artificial Intelligence and Democratic Norms - Meeting the Authoritarian Challenge, Sharp Power and Democratic Resilience Series, The National Endowment For Democracy (August 2020), <https://www.ned.org/sharp-power-and-democratic-resilience-series-artificial-intelligence-and-democratic-norms/>

¹⁶⁹ See also: 20200917_IETC Hearing with Chairman Eric Schmidt: "Interim Review of the National Security Commission on AI" <https://youtu.be/USEKVNSf4ol?t=862>.

¹⁷⁰ See: <https://edition.cnn.com/2020/12/31/europe/eu-bad-2020-2021-analysis-intl/index.html>

opinions between the US and the EU on antitrust, digital tax and digital trade¹⁷¹, and consensus on IP policy, ethics, cybersecurity and the need for global value-based standards that respect democratic freedoms, human rights and the rule of law. On the other hand, it can be quite healthy to have mutual differences, and a varied pallet of perspectives within a partnership.

Moreover, who are we to pursue worldwide, culturally sensitive norms and standards? Could this be perceived by other countries as undesirable technologically expansionist behaviour? Will excessive standardization, certification and benchmarking have ramifications on rapid innovation, global competition and consumer welfare?

Brexit has made it painfully clear how difficult it is to agree on even the most trivial affairs. The question is whether the barriers to cooperation will be removed, just because a new wind is blowing from White House.¹⁷²

In conclusion: political support to realize our ideal is a precondition for success. Preferably not in a weakened compromise form, but in a manner that reflects the power of the technology and the interests at stake. Instead of an isolationist MAGA approach, policy makers on both sides of the spectrum need to see the bigger picture and the urgency of the issues at hand. And reach out

¹⁷¹ See: <https://www.politico.eu/article/eu-to-us-president-elect-joe-biden-lets-be-tech-allies/>

¹⁷² See also: <https://www.politico.eu/article/eu-rope-us-technology-drifting-joe-biden/>

¹⁷³ See Kop, *supra* note 21 and Mamudu HM, Studlar DT. Multilevel Governance and Shared Sovereignty: European Union, Member States,

to nations that historically share our values and that demonstrably meet the democratic conditions set by the Alliance to qualify for membership.

With existential challenges ahead of us, normative choices must be made. We cannot get there with transactional politics and trade deals alone. We have to bring the best of both worlds together. A combination of normative choices - which are contextual, culturally sensitive and in constant flux - and Realpolitik is the key. Making the right choices today can result in the lasting partnerships we need to respond to the big questions we face. Partnerships based on mutual trust, strategic autonomy and shared sovereignty.¹⁷³ Partnerships that acknowledge the need for regulatory cooperation and a values-based approach.

5. Are We Democratic Enough Ourselves?

Let's see if we can approach this matter from other, socio-critical perspectives.

First, are the Chinese the real threat, or is it us? Are we really democratic enough ourselves?¹⁷⁴ Is making the distinction between the democratic and the authoritarian model the correct line of thinking, the proper

and the FCTC. *Governance (Oxf)*. 2009;22(1):73-97. doi:10.1111/j.1468-0491.2008.01422.x

¹⁷⁴ See for example: <https://www.wbur.org/on-point/2021/03/09/vaccine-passports-public-health-tool-or-invasion-of-civil-liberties>

approach for our proposed response to the identified challenges? Are technology and data capitalism coupled with the wrong kind of self-regulation causing filter bubbles, fake news and racial bias?¹⁷⁵ In other words, could technology that originated from Western online platforms such as Facebook, Amazon, Google and Twitter be the real source of danger? Are the behemoth platforms, with market dominance and lobbying power greater than countries, menacing our democracy? In general, absent regulation, the tech platforms have corporate social responsibility and should adopt an Apollonian mindset towards responsible entrepreneurial ideology, world view and philosophy of life, instead of a Dionysian attitude.¹⁷⁶

One can argue whether the harmful societal influence of the social platforms was caused by naive idealism from Silicon Valley, or by unrealistic price and profit expectations of Wall Street.¹⁷⁷ Or by a combination thereof. In this view, the algorithms¹⁷⁸ have become less democratic not so much as a consequence of the wrong corporate ideology, but because of the increasing pressure that

shareholders are putting on tech companies.¹⁷⁹ Thus, the system is to blame.

But can you be a role model for the rest of the world this way? Are the dangers of our privatized technology governance model not as threatening, or even more dangerous to our society than the predictable authoritarian technology governance model could ever be? Is there an enemy within, that stands at the cradle of excesses like the Capitol Insurrection?¹⁸⁰ Is the privatized power over the digital world a similar existential challenge, for which solutions must be developed? The answer appears to be in the affirmative. Democratic countries themselves have serious internal problems.

Moreover, there is no empirical evidence that AI will endanger democracy and reinforce authoritarianism, totalitarianism or even fascism, since AI is ideologically neutral.¹⁸¹ That said, shouldn't we better use machine values instead, since human values create biases in data and algorithms, fake news and conspiracy theories?¹⁸²

Be that as it may, from a higher level, a strategic democratic alliance can provide a

¹⁷⁵ See: Marietje Schaake, How democracies can claim back power in the digital world, MIT Technology Review, September 29, 2020, <https://www.technologyreview.com/2020/09/29/1009088/democracies-power-digital-social-media-governance-tech-companies-opinion/>

¹⁷⁶ Mauritz Kop, *AI & Intellectual Property: Towards an Articulated Public Domain*, 28 *Tex. Intell. Prop. L. J.* 297 (2020)

¹⁷⁷ See: <https://www.technologyreview.com/2020/12/03/1012797/fair-value-fixing-the-data-economy/>

¹⁷⁸ See also: <https://yjolt.org/blog/legality-artificial-intelligence-contact-tracing-stop-corona-virus-us>

¹⁷⁹ See against this background: <https://www.netflix.com/nl/title/81254224>

¹⁸⁰ See: <https://www.npr.org/2021/02/09/965472049/the-capitol-siege-the-arrested-and-their-stories>

¹⁸¹ Ünver, *supra* note 13.

¹⁸² See in this light also: <https://www.wired.com/story/opinion-ai-is-an-ideology-not-a-technology/>

counterbalance to both the free-market capitalism based privatized digital governance model, and the authoritarian model. In the duel for AI dominance and the battle to be the first to build a functioning multi-purpose quantum computer, the West desperately needs the Tech Giants from the Silicon Valley and Massachusetts innovation clusters.

6. Two Dominant Tech Blocks

Currently, two dominant tech blocks exist: the US and China. The blocks have incompatible political systems. It is a battle between ideologies.¹⁸³ Liberal democracy versus authoritarianism. Free market capitalism versus surveillance capitalism. Europe stands in the middle, championing a legal-ethical approach to tech governance. Its Member States often divided when it comes to Beijing: 12 of them participate in Xi Jinping's Belt and Road program.

It is of crucial strategic importance to proactively consider potential alternative scenarios.¹⁸⁴ Future scenarios in which our desired coalition of democratic countries did not materialize for whatever reason. We can use scenario planning for this. Scenario planning, or scenario analysis, is the development, comparison and anticipation of

probable future scenarios, together with short- and longer-term transitions.¹⁸⁵ Impending scenarios meant to be used as thinking instruments.

Alternatives to the creation of a strong democratic Strategic Tech Alliance are no alliance or different alliances. Each scenario could bring both (trade) war and peace to the world. Please note that establishing a league of like-minded democratic countries does not guarantee winning the race for AI and quantum supremacy. Moreover, competition and rivalry between blocks could incentivize exponential innovation. The race for AI supremacy is not a zero-sum game.

Does one rule out the other? Could the US or the EU be both a partner and rival of China through smart partnerships? In theory, it is a position that both the US and the EU could take. In tandem with bolstering alliances with our allies, we should -to a certain extent- be open to dialogue and cooperation with the regimes. We also have to consider an unthinkable alliance of EU-China-Russia 'against' a pact between countries like US/Canada/UK/Israel/Australia/India/South-Korea/Japan.¹⁸⁶

Another scenario is a protracted Cold War for AI Supremacy with no winner between

¹⁸³ See also: <https://edition.cnn.com/2021/03/04/asia/xi-jinping-china-npc-successor-intl-hnk/index.html>

¹⁸⁴ See also: <https://www.atlantic-council.org/event/the-global-quest-for-digital-sovereignty/>

¹⁸⁵ Ron Bradfield, George Wright, George Burt, George Cairns, Kees Van Der Heijden, The

origins and evolution of scenario techniques in long range business planning, Futures, Volume 37, Issue 8, 2005, Pages 795-812, ISSN 0016-3287, <https://doi.org/10.1016/j.futures.2005.01.003>.

¹⁸⁶ See also: <https://www.cnas.org/publications/video/navigating-the-china-russia-partnership>

the US and China.¹⁸⁷ A no winner takes all scenario would eventually mark the Splinternet.¹⁸⁸ On the one hand a China led internet, characterized by a top-down approach to tech. It would comprise of countries that adopt Chinese apps. Its rival would be a US influenced internet, including countries that adopt US built platforms and apps. From the server level, cloud computing and AI all the way down to the phone operating system level. Cyberbalkanization could result in two parallel worlds, each with distinct divisions regarding technology, trade and ideology. In practice, this implies two opposing ecosystems would exist, each using its own standards and architectures that are incompatible with one other.

In the event China wins the race for AI and quantum, it will have the power to overthrow the EU and the US.¹⁸⁹ The world would see a new era of authoritarian surveillance capitalism. In the case that a strategic partnership of democratic countries led by the US and the EU will prevail, it may well coerce China to adopt Humanist values.

To prevent China Standards 2035,¹⁹⁰ we need a coalition of democratic countries that bakes its values into its technology and that sets worldwide interoperability standards for telecommunications, AI & quantum infrastructures.

¹⁸⁷ See also: <https://edition.cnn.com/2021/01/05/europe/uk-aircraft-carrier-strike-group-intl-hnk-mil/index.html>

¹⁸⁸ See: Mark A. Lemley, The Splinternet (July 30, 2020). Stanford Law and Economics Olin Working Paper #555, Available at SSRN: <https://ssrn.com/abstract=3664027>

7. Harms of Doing Nothing

The described advantages of the establishment of an alliance must be weighed against disadvantages, unintended consequences and the harms of doing nothing.

First, no alliance means fragmentation and division, without synergetic effects. A lack of action entails less chance of winning the race for tech dominance and securing the chance to set and control global standards. Standards that preserve democratic values. The danger of global autocratic values in technology and infrastructure increases in this analysis, because there is no *en bloc* counterbalance to emerging countries such as China, the country of the large numbers of consumers, hordes of AI talent, and huge amounts of machine learning training data, regurgitated by labelling farms. China has massive government budgets for the development of smart algorithms and quantum technology applications. Currently it's everybody for himself; that won't help us win the race. We need an alliance instead of division.

Second, quantum technology enhances AI. Together with blockchain it promises machine learning on steroids. Quantum and AI hybrids will give to the world a new perspective of science itself. In this context, it is

¹⁸⁹ See also: <https://edition.cnn.com/2021/03/05/china/china-world-biggest-navy-intl-hnk-ml-dst/index.html>

¹⁹⁰ See: <https://www.cnbc.com/2020/04/27/china-standards-2035-explained.html>

crucial to raise awareness of their incredible potential for good, and their anthropogenic risks. The Fourth Industrial Revolution will bring about a world in which anything imaginable to improve, or worsen the human condition, can become reality.

Authoritarian countries obtaining this powerful technology and using it against us, poses serious national cybersecurity (cyberwarfare, hacking) threats.¹⁹¹ More importantly, the regimes would have the ability to impose their non-democratic values on us through technological expansionism. From our liberal-democratic viewpoint, this could lead to a dystopian scenario. AI driven facial recognition systems used for shadowing and social credit systems would become the standard. Surveillance machines are a dictator's dream. Authoritarian a-moral *machina sapiens* will take over creation and invention. Privacy, mental security and freedom of thought will become a distant memory.

Our society will be better off when we forge Democratic Alliances. A united democratic tech block has a greater chance of winning the race for AI & quantum dominance.

Third, long term risks of underinvesting in 4IR technology are no less than existential. The US needs to invest heavily in safe & responsible AI and quantum. The market

cannot pull this off on its own. The state should take the lead and launch a mission oriented, 2030 US Standards plan, backed by large-scale funding.¹⁹² This plan should be sharply demarcated, and executed by golden triangle, public-private partnerships. These partnerships can be based on the triple helix innovation model, which guarantees synergistic effects between government, academia and business.

The portrayed advantages of bolstering an alliance, and actively shaping technology for good evidently outweigh the harms of remaining passive or indecisive. It is critical that the US does not hang back in a never-ending balancing of stakeholder concerns but that it is confident in formulating a vision and focussed in accomplishing its well defined national and global policy objectives. By doing nothing the US will fall behind economically. The US and the EU should set out the path along transatlantic lines and guide their democratic allies toward a Strategic Tech Alliance.¹⁹³

8. Regulating 4IR Technology

Regulating emerging technology is an unending endeavour. It is an ongoing, cyclic process that follows the lifespan of the technology and its implementation. How should Democratic countries construct regulatory

¹⁹¹ See: <https://jolt.law.harvard.edu/digest/the-solarwinds-software-hack-a-threat-to-global-cybersecurity>

¹⁹² See also: <https://www.reuters.com/article/us-health-coronavirus-economy-breakingview/idUSKBN29Y219>

¹⁹³ See also: <https://edition.cnn.com/2021/02/19/politics/joe-biden-for-foreign-policy-speech/index.html>

solutions that are tailored to the exponential pace of innovation in the Fourth Industrial Revolution?

A crucial first step is to map the risks and chart culturally sensitive ethical, legal and social implications (ELSI), per 4IR technology.¹⁹⁴ Then, universal principles, or core requirements, that manage these ethical, legal and social issues and risks should be considered, exchanged and discussed.¹⁹⁵

The second step is to implement agile, flexible governance solutions that can quickly adapt and respond to sudden changing conditions and societal demands.¹⁹⁶ In this light, the construction of binding technology specific legal-ethical frameworks, accompanied by soft law instruments such as risk-based technology assessments¹⁹⁷, audits and legal sandboxes would be an essential regulatory intervention. Again, we have to differentiate, and make this regulatory effort per emerging 4IR technology. For example, a legal-ethical framework for AI should

consist of joint, agreed upon core horizontal rules that are binding across industries.¹⁹⁸

Step 3 is to complement these overarching rules by vertical, industry-specific requirements -including self-regulation- that fit in the existing Quality Management Systems for economic sectors, or domains, such as the Food industry, the Health sector, Energy, Finance and so on.¹⁹⁹ The AI legislative approach can be applied, or linked to quantum technology and VR, to a certain level.²⁰⁰ Naturally, the distinctive physical characteristics of quantum technology demand for an extra set of core horizontal and for additional sector specific vertical rules.²⁰¹ For each technology, the goal is to harmonize quintessential core rules, preferably by means of codification in a Declaration or a Convention.

As mentioned earlier, shared (interoperability) standards, benchmarks and certification

¹⁹⁴ Kop, *supra* note 22.

¹⁹⁵ Mauritz Kop, *Regulating Transformative Technology in The Quantum Age: Intellectual Property, Standardization & Sustainable Innovation*, 2 TTLF Newsletter on Transatlantic Antitrust and IPR Developments Stanford-Vienna Transatlantic Technology Law Forum, Stanford University 2020, <https://law.stanford.edu/publications/regulating-transformative-technology-in-the-quantum-age-intellectual-property-standardization-sustainable-innovation/>

¹⁹⁶ See: Stefaan Verhulst, *Introducing the Digital Policy Model Canvas*, <http://thego-vlab.org/introducing-the-digital-policy-model-canvas/>; and World Economic Forum, *White Paper Digital Policy Playbook 2017: Approaches to National Digital Governance*,

http://www3.weforum.org/docs/White_Paper_Digital_Policy_Playbook_Approaches_National_Digital_Governance_report_2017.pdf.

¹⁹⁷ See: Mauritz Kop, *AI Impact Assessment & Code of Conduct*, European AI Alliance (European Commission), May 29, 2019, <https://future.ec.europa.eu/en/european-ai-alliance/best-practices/ai-impact-assessment-code-conduct> and <https://www.iaia.org/wiki-details.php?ID=26> and <https://www.jstor.org/stable/4200654?seq=1>

¹⁹⁸ Kop, *supra* note 21, 22 and 59.

¹⁹⁹ See Kop, *supra* note 22.

²⁰⁰ For a detailed description of linking AI to quantum considering regulation of 4IR technology, see: Kop, *supra* note 22.

²⁰¹ See Kop, *supra* notes 22 and 59.

play a vital role in regulating 4IR technology.²⁰²

The envisioned horizontal-vertical legal-ethical framework should address the identified risks associated with the technology, with enforcement mechanisms tailored to low, mid and hi-risk applications.²⁰³ In addition, the framework should contain incentives for sustainable innovation.²⁰⁴ These incentives include balanced intellectual property laws²⁰⁵, mission-oriented approaches driven by moon shot thinking such as the cold war Apollo project, as well as rules for healthy competition that prevent winner-takes-all effects and give room to both technology transfer and the creation of vibrant start-up ecosystems. Besides 'environmentally friendly', the term 'sustainable' also pertains to socially inclusive, human centred digitization, democracy, rule of law, and human rights.²⁰⁶ Lastly, the binding horizontal-vertical rules should be flanked by quasi legal instruments such as technology road mapping tools.²⁰⁷

Technology road mapping tools like *ex ante* impact assessments, best practices and moral guides can help raising awareness of the societal impact of 4IR technology.²⁰⁸ These concrete tools can assist us in making sure we are modelling technology for good.²⁰⁹ Moreover, these guides can offer support to companies in their endeavour to comply to, or anticipate on legal, technical and agreed upon ethical requirements.²¹⁰ To a certain degree, flexible tools can even be used as alternatives for non-existent or insufficient hard laws.²¹¹ Thus, risk-based AI & quantum impact assessments, performed by multidisciplinary audit teams, can assist in validating that real world AI, data, quantum & VR driven products and services remain legal, ethical, social and technically robust throughout their life-cycle.²¹²

Following these steps, risks can be dealt with and the positive aspects of the technology can be employed to make the world a better place.²¹³

²⁰² Kop, *supra* note 12.

²⁰³ Kop, *supra* note 21 and 22.

²⁰⁴ Kop, *supra* note 21, 22 and 59.

²⁰⁵ See: Mauritz Kop, *The Right to Process Data for Machine Learning Purposes in the EU* (June 22, 2020). Harvard Law School, Harvard Journal of Law & Technology (JOLT) Online Digest 2021, Forthcoming, <https://ssrn.com/abstract=3653537>

²⁰⁶ See also: Kop, *supra* note 20.

²⁰⁷ See also: Kop, *supra* note 59.

²⁰⁸ See Kop, Kop, *supra* notes 21, 22 and 40.

²⁰⁹ See for example: <https://www.scientificamerican.com/article/can-ai-identify-toxic-online-content/> and <https://news.stanford.edu/2021/03/08/assessing-regulatory-fairness-machine-learning/>

²¹⁰ See also: CAHAI feasibility study on AI legal standards, <https://www.coe.int/en/web/artificial-intelligence/-/the-feasibility-study-on-ai-legal-standards-adopted-by-cahai>

²¹¹ See also: Kop, *supra* note 22, Mark A. Lemley, *The Contradictions of Platform Regulation* (February 3, 2021). Available at SSRN: <https://ssrn.com/abstract=3778909> and <https://www.technologyreview.com/2021/01/15/1016183/ai-ethics-startups/>

²¹² Kop, *supra* note 61.

²¹³ Note that innovation by itself cannot fix all the problems of humanity, see: Ünver, *supra* note 13.

Please note that being an authoritarian regime isn't always a bad thing. The regimes can be far more effective in battling climate change, since they have the luxury to avoid lengthy multi-stakeholder debates.²¹⁴ Consensus is not needed. In that respect they excel in centralization, decisiveness, efficiency, and speed. Democratic policy makers should build on these healthy habits.²¹⁵

In other words, being authoritarian doesn't mean one can't be successful in addressing the big questions we face. Countries don't need to be democratic for that.

9. Conclusion

The race for AI and quantum dominance isn't just a competition in technology and market power. It is as much a competition in norms, standards, principles and values.²¹⁶ It is expected that the prevailing party will set global technology requirements/guidelines for decades to come.²¹⁷ Whoever wins the race for AI & quantum supremacy will impose their values on the rest of the world through the distribution of their technology. These technologies will become the dominant platforms.

We are living in a Golden Age of exponential technological innovation. Legal problems regarding human rights, algorithmic bias

and built-in discrimination, data access, sharing and re-use may now be assumed to be generally known to policy makers. We should change the story. We must urgently solve these problems and set global technology standards together. Like-minded countries with compatible political systems must collaborate on socio-economic and ethical issues surrounding AI, data, and quantum technology. We have an ideological commitment to bake our democratic values into our intelligent systems. This way, society can benefit from the benevolent side of the 4IR.

What should democratic governments do?

To prevent authoritarianism from gaining ground, governments should do three things: (1) form a broadly scoped democratic Strategic Tech Alliance, (2) set worldwide core rules and standards for AI, quantum, 6G and VR, and (3) embed our common norms, principles, values into the design of our technology.

What can you do? You can participate by convincing your congresswomen or congressmen that the time is ripe to bolster a strong international Strategic Tech Alliance. Besides that, you can make conscious sustainable living choices about products and services that you purchase and use in your everyday life, and about (the origin & environmental footprint of, and democratic

²¹⁴ See also: <https://www.brookings.edu/blog/order-from-chaos/2020/12/23/the-risk-of-john-kerry-following-his-own-china-policy/>

²¹⁵ See also: <https://www.technologyreview.com/2021/01/01/1015533/covid->

[lessons-for-climate-change-emissions-renewables/](https://www.brookings.edu/blog/order-from-chaos/2020/12/23/the-risk-of-john-kerry-following-his-own-china-policy/)

²¹⁶ Kop, *supra* note 21.

²¹⁷ See: <https://www.ces.tech/Articles/2020/Whoever-Leads-AI-Will-Lead-the-World.aspx>

values embedded in) the technology utilized in those products and services. A better planet starts with you. You can also help by spreading awareness about the design decisions people around you -programmers, data scientists, managers, evangelists and business-leaders- can make. Conscious decisions that ensure 4IR technology is implemented in a responsible and sustainable manner.

The architecture of intelligent systems should articulate values that we consider important as a society, from the first line of code. Following this path, we can avoid a dystopian future and make technology a greater force for good.

Other Developments

European Union

How to Ensure National Security in the New Media Age

By Gabor Szecsi

Not too long ago, making a trans-Atlantic telephone call to colleagues or loved ones required scheduling and operator assistance, and it wasn't inexpensive. Today, VoIP²¹⁸ services allow us to speak with someone across the globe without third-party assistance and without advance planning. No matter how far apart people are physically, they can still easily connect, collaborate and remain close to each other in

the cyberspace; thanks to the facility of the Internet²¹⁹.

Nevertheless, evil always tries to find the way to spoil the blessing. Social media and other communication applications have become a significant source of criminal activities and national security threats. Authoritarian states can use these platforms to influence and weaken liberal democratic societies²²⁰. Unsecured sharing of information makes individuals and society vulnerable and susceptible to criminal acts, unfair business practices, or terrorist attacks. National governments now face the new challenge of countering foreign government influence, cybercriminals, and cyberterrorists while maintaining freedom of communication and the free flow of ideas.

In an effort to curb foreign government influence, Australia²²¹ and India²²², for example, restricted the operation of various Chinese Internet companies. The European Union²²³

²¹⁸ Voice over Internet Protocol. It is an inexpensive way to make international phone calls. For example, WhatsApp, Skype, and WeChat offer Voip services.

²¹⁹ U.S. Supreme Court has also acknowledged that cyberspace is the most important place for the exchange of ideas. *Packingham v. North Carolina*, 137 S.Ct. 1730, 1735 (2017)

²²⁰ Submission to the Senate [of the Parliament of Australia] Select Committee on Foreign Interference through Social Media: Dr Jake Wallis and Mr Thomas Uren are Senior Analysts at the Australian Strategic Policy Institute (ASPI).

²²¹ Freedom of Information Disclosures; <https://defence.gov.au/FOI/decisions/DisclosureLog201920.asp> February 15, 2021; Australian Department of Defense banned for its

personnel to download WeChat to their mobile device.

²²² India makes ban on TikTok, WeChat, 57 other Chinese apps permanent published by South China Morning Post, January 26, 2021; <https://www.scmp.com/news/asia/south-asia/article/3119227/india-makes-ban-tiktok-wechat-57-other-chinese-apps-permanent> February 15, 2021

²²³ The Court held that the US does not provide for an *essentially equivalent*, and therefore sufficient, level of protection as guaranteed by the GDPR and the CFR. As a result of the Court's decision, EU companies can no longer legally transfer data to the US based on the Privacy Shield framework. Companies that continue to transfer data on the basis of an invalid mechanism risk a penalty of €20 million or 4 % of their global turnover, pursuant to Article 83(5)(c) GDPR.

and the United States²²⁴ also attempted to counter foreign government's surveillance programs²²⁵. The EU characterized the problem as a data protection issue, while the U.S. characterized the problem as a national security issue. This article analyses the EU and the U.S. efforts to prevent foreign government entities from accessing their citizens' private and proprietary information.

The American approach: Throwing the baby out with the bathwater

Foreign governments can use U.S. citizens' user data collected by social media

[https://www.europarl.europa.eu/Reg-DATA/etudes/ATAG/2020/652073/EPRS_ATA\(2020\)652073_EN.pdf](https://www.europarl.europa.eu/Reg-DATA/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf) February 16, 2021

²²⁴ see: E.O. 13971 of Jan 5, 2021,

<https://www.federalregister.gov/documents/2021/01/08/2021-00305/addressing-the-threat-posed-by-applications-and-other-software-developed-or-controlled-by-chinese>; E.O. 13943 of Aug 6, 2020

<https://www.federalregister.gov/documents/2020/08/11/2020-17700/addressing-the-threat-posed-by-wechat-and-taking-additional-steps-to-address-the-national-emergency> February 15, 2021

²²⁵ More on U.S. surveillance laws: National Security Act of 1947, Omnibus Crime Control and Safe Streets Act of 1968 (aka "Wiretap Act"), Foreign Intelligence Surveillance Act (FISA) of 1978, Electronic Communications Privacy Act of 1986, Patriot Act of 2001, Communications Assistance for Law Enforcement Act of 2006, Patriot Sunsets Extension Act of 2001, Protect America Act of 2007, USA Freedom Act of 20015, and the 4th Amendment of the Constitution of the United States.

companies²²⁶ to distort political discourse, incite criminal acts, encourage terrorism, influence voting behavior or alter electoral outcomes²²⁷. The president of the United States focused solely on national security concerns when he tried to cope with the problem. The International Emergency Economic Powers Act²²⁸ (IEEPA) and the National Emergencies Act²²⁹ empowers the president to regulate a subject, should an unusual and extraordinary threat arise²³⁰.

Invoking his right under IEEPA, the president declared an emergency and issued two Executive Orders that banned WeChat and TikTok. Later, a third Executive Order banned a number of other Chinese applications as well. The companies sued the U.S.

²²⁶ E. O. 13943 of August 6, 2020; Social media applications like WeChat and TikTok are designed to capture vast swath of information.

²²⁷ Submission to the Senate [of the Parliament of Australia] Select Committee on Foreign Interference through Social Media: Dr Jake Wallis and Mr Thomas Uren are Senior Analysts at the Australian Strategic Policy Institute (ASPI).

https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_through_Social_Media/ForeignInterference/Public_Hearings, February 15, 2021

²²⁸ 50 U.S.C. 1701 *et seq.* This section empowers the President to counter any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States. Historically, the IEEPA gave broad power to the president to deal with "unusual and extraordinary threat" to the United States.

²²⁹ 50 U.S.C. 1601 *et seq.*; See also 3 U.S. Code § 301 - General authorization to delegate functions; publication of delegations.

²³⁰ See also 3 U.S. Code § 301 - General authorization to delegate functions; publication of delegations.

government, the litigation is pending. The Executive Orders were intended to prevent the gathering of American user data that might be shared, voluntarily or involuntarily, with the Chinese government.

However, the orders implemented by the Department of Commerce²³¹ singled out a few social media companies, and these orders essentially prevented the Chinese-American community to interact with their families, friends, and business partners in China. This drastic, all-out approach shut down the entire medium of communication and deprived a large group of U.S. citizens from being able to effectively communicate with their peers. Not only could the constitutionality of the president's action be disputed, but also it begs the question whether an absolute and total suppression of a medium of communication would be aligned with the values of the western democracies.

The most cherished and respected constitutional right was sacrificed for national security

²³¹ 85 FR 60061: Identification of Prohibited Transactions to Implement Executive Order 13942 and Address the Threat Posed by TikTok and the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain; <https://www.federalregister.gov/documents/2021/01/08/2021-00305/addressing-the-threat-posed-by-applications-and-other-software-developed-or-controlled-by-chinese>, February 15, 2021

²³² *City of Ladue v. Gilleo*, 512 U.S. 43 (1994) <https://supreme.justia.com/cases/federal/us/512/43/> February 15, 2021

²³³ Case: 20-16908, 11/27/2020, ID: 11907964, DktEntry:35, U.S. WeChat Users Alliance, Chihou Inc.. Brent Coulter, Fangyi Duan, Jinneng

Freedom of speech protects the free flow of ideas. Whenever the government seeks to regulate freedom of speech, the Court will weigh the importance of this right against the government interest. Although the president's action was intended to regulate the platform only, the government action inevitably affected the communication itself.²³² Hence, the validity of the Executive Orders are a function of the freedom of speech. When analyzing the constitutionality of a government action regarding freedom of speech the first question to ask is whether the regulation is content based or content neutral. Here, WeChat argues that the Executive Order is content based because the president's action singles out an application used predominantly by the Chinese community.²³³ If the court accepts this argument the Executive Order is subject to strict scrutiny, and the government will likely lose the case²³⁴.

Alternatively, if the court found that the Executive Orders are content neutral, they would be subject to a three-part test²³⁵ that,

Bao, Elaine Peng, and Xiao Zhang v. Donald J. Trump.

²³⁴In case of strict scrutiny, a government has to prove that the government action is necessary to achieve a compelling government interest, and there is no less restrictive means to accomplish the government's objective. The government action likely fails if strict scrutiny applies.

²³⁵ *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622 (1994) In case of content-neutral government regulation, the court uses the following three-part test: First, the regulation must serve a significant government interest. Second, the regulation must be narrowly tailored to serve that government interest. Finally, the

among other things, requires the regulation to be narrowly tailored. Executive Orders that impose a total and absolute ban on speech are hardly narrowly tailored.

The reasonableness of the regulations can also be contested. An overly broad regulation will not be upheld because the purpose of freedom of speech is to encourage the free flow of ideas.²³⁶ The Supreme Court held unconstitutional a local ordinance that prohibited speech that “in any manner” interrupts a police officer in the performance of her duties.²³⁷ Here, the Executive Order prohibited “any transaction” that is related to WeChat by “any person,” or with respect to “any property,” subject to the jurisdiction of the United States.” The Executive Orders seem similarly overbroad to the local ordinance that was invalidated by the Supreme Court.

These constitutional concerns put the government in an incredibly weak position before the Court. Even if the intent and purpose of the legislation have their merits, the execution resulted in three misguided, poorly written Executive Orders that will likely fail to pass the constitutional

state must leave open alternative channels for communicating information.

²³⁶ *Virginia v. Hicks*, 539 U.S. 113 (2003)

²³⁷ *Houston v. Hill* 482 U.S. 451 (1987)

²³⁸ No. 20-16908D.C. No. 3:20-cv-05910-LB Northern District of California, San Francisco Defendants-Appellants’ unopposed motion to hold this case in abeyance was Granted on February 11, 2021. The new administration has asked the court to halt the proceeding until the Department of Commerce reviews certain recently issued agency actions, including

muster²³⁸.

In summary, lawsuits filed by WeChat and TikTok demonstrate that there is a very strong relationship between national security interests and freedom of speech, and neither subject should be ignored when regulating social media. The Executive Orders nicely illustrate that an exclusively national security-oriented approach would likely infringe on freedom of speech.

Conversely, the EU turned to the fundamental right of privacy to prevent foreign government surveillance on EU citizens’ private and proprietary information.

The European approach: National security through privacy protection

Interestingly, the EU deems American privacy protection inadequate, but WeChat is not prohibited or otherwise restricted to operate in the EU. Nevertheless, the EU also recognized the potential threat posed by foreign entities who might get access to European citizens’ personal or proprietary information. That was the exact reason why the

WeChat mobile application at issue. The review should consider two issues. First, a government has a constitutional obligation to respect freedom of speech which was overlooked by the drafters of the Executive Order. Second, regardless of the possible invalidity of the order, the government correctly recognized the potential national security threat posed by social media and other communication platforms. This threat must be addressed in a manner consistent with the law and western democratic values.

European Court of Justice invalidated the Privacy Shield framework with two landmark decisions, *Schrems I* and *II*²³⁹. The European Court of Justice observed that U.S. data protection level is inadequate partially because of the U.S. government's surveillance program.²⁴⁰

Essentially, the justification of WeChat and TikTok Executive Orders were exactly the same as the justification of the Privacy Shield invalidation. The TikTok order states the following: "This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information..." Thus, the EU is concerned that the U.S. government gets access to EU citizens' personal and proprietary information while the U.S. is concerned that the Chinese Communist Party gets access to Americans' personal and proprietary information.

²³⁹ The CJEU found that European Commission's adequacy determination for Privacy Shield is invalid for two main reasons. First, the court found that U.S. surveillance programs, are not limited to what is strictly necessary and proportional, and thus it does not meet the requirements of Article 52 of the EU Charter on Fundamental Rights. Second, the court determined that EU data subjects lack actionable judicial redress with regard to U.S. surveillance as required by Article 47 of the EU Charter. Learn more about Schrems decisions at <https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/> February 16, 2021

²⁴⁰ See more on Privacy Shield at <https://www.privacyshield.gov/welcome> February 16, 2021

²⁴¹ Article 8 of Convention for the Protection of Human Rights and Fundamental Freedoms. ETS No. 005, 1950;

If the European Court of Justice had followed the American approach, it would have banned Facebook in the EU. Instead, the Court had a different approach; it turned to the fundamental right of privacy. Article 8 of European Convention on Human Rights guarantees the right to respect for private and family life, home, and correspondence.²⁴¹ People have a right to protection of their private sphere against intrusion from others, especially from state actors.²⁴² Thus, the European fundamental right of privacy guarantees that state actors or other people do not get unauthorized access to their private information. Since this unauthorized access itself poses the national security threat, ensuring the right of privacy set forth in the European Convention on Human Rights would reduce national security threat as well.

As a solution, the EU limited transfer to untrusted third countries²⁴³. The default rule in

²⁴² See Article 12 of the United Nations Universal Declaration of Human Rights (UDHR) of 1948,

<https://www.un.org/en/universal-declaration-human-rights/index.html> February 18, 2021

²⁴³ Article 45 of the European Parliament and Council of European Union (2016) Regulation (EU) 2016/679. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN> (Accessed: 2 December 2019). February 16, 2021 ²⁷ Max Schrems v. Data Protection Commissioner (CJEU - "Safe Harbor"), <https://epic.org/privacy/intl/schrems/> February 16, 2021 ²⁸ Article 45 of the European Parliament and Council of European Union (2016) Regulation (EU) 2016/679. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN> (Accessed: 2 December 2019). February 16, 2021

the European Union prohibits cross-border data transfers.²⁷ A transfer of personal data to a third country or an international organization may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection.²⁸ If the country does not have an adequate level of protection, certain alternative assurances must be in place for the permission of data transfer in that country.

The European Union prefers to keep the personal and proprietary information within the EU borders, where it can exercise more supervision, ensure data protection, and prevent espionage. The European approach suggests that it is more difficult for foreign governments to compel or exert force on a company to disclose personal data if the data is not stored under the foreign government's jurisdiction. Also, the European authorities can counter espionage more effectively if the data remains in the EU. Therefore, what guarantees data privacy inevitably reduces national security threat.

Conclusion

In summary, there are two different approaches on each side of the Atlantic to address the same problem. The European approach shows that data privacy and national security have the same ultimate objective. Namely, to prevent the citizen's personal and proprietary information from falling into the wrong hands.

The American action focused only on national security concerns and led to a violation of the Constitution. Conversely, the EU used a fundamental right, the right of privacy, to achieve the same goal. The European solution is less intrusive and does not have any effect on speech. Thus, it would pass the constitutional muster in the U.S. as well.

Therefore, a future U.S. legislation to prevent online national security threats and cybercriminal activities should consider the enhancement of privacy protection.

Copyright © 2021 contributors. This issue and the previous issues of the Transatlantic Antitrust and IPR Developments can be accessed via its webpage on the Transatlantic Technology Law Forum website.