# THE INTERGOVERNMENTAL ORGANISATIONS IN-HOUSE COUNSEL JOURNAL

**ISSUE 1** - MAY 2020

ISSN 2632-9727 (Online)

ALIFDO

The Law Journal of the Association of Lawyers in Intergovernmental Finance and Development Organisations

www.alifdo.com

## The Intergovernmental Organisations In-House Counsel Journal

The Intergovernmental Organisations In-house Counsel Journal is the law journal of the Association of Lawyers in Intergovernmental Finance and Development Organisations (ALIFDO) Ltd. It is published electronically once every two years and is free of charge to the public.

The purpose of the journal is to provide a platform for ALIFDO members, academics and other practitioners, to identify and explore topics of interest to lawyers working for international organisations committed to finance or development, and to those who are interested in the work of these organisations.

## Disclaimer

The Intergovernmental Organisations In-House Counsel Journal (IOICJ) and ALIFDO, as well as their agents and licensors make no representations or warranties whatsoever as to the accuracy, completeness or suitability for any purpose of the content of this journal and disclaim all such representations and warranties whether express or implied to the maximum extent permitted by law. Any views expressed in the articles are the views of the authors and may not necessarily represent the views of the authors' affiliated organisations.




Special thanks to Jenny Liang, from Harvard University, and to the following lawyers from the European Bank for Reconstruction and Development: Yunus Ernazarov, Muge Minareci, Dionysis Diamantatos, Begum Naz Bayirbas and Sher Yunusov.


ALIFDO

# About ALIFDO

ALIFDO is an individual membership-based organisation for lawyers working, in whatever capacity, for intergovernmental organisations committed to finance or development. For more information, please visit ALIFDO's website: www.alifdo.com

As of the date of publication of this Journal, ALIFDO has individual members at the following organisations:

- The International Monetary Fund
- The Black Sea Trade and Development Bank
- The OPEC Fund for International Development
- The European Bank for Reconstruction and Development
- The Asian Development Bank
- The Global Fund
- The Asian Infrastructure Investment Bank
- The Caribbean Development Bank
- The Council of Europe Development Bank
- The International Fund for Agricultural Development
- The Green Climate Fund
- The Nordic Investment Bank
- The New Development Bank
- The International Development Law Organisation
- The Inter-American Development Bank Group
- The International Finance Corporation
- The World Bank (Finance, Innovation & Competitiveness Global Practice)
- The Multilateral Investment Guarantee Agency
- GAVI, The Vaccine Alliance
- The African Development Bank

An up-to-date listing of organisations where ALIFDO has individual members can be found at www.alifdo.com/membership

**Subscriptions and Future Issues**

The IOICJ is published online on ALIFDO's website at www.alifdo.com/the-intergovernmental-organisations-in-house-counsel-journal

Print editions are currently not available.

To be added to the IOICJ's mailing list, please go to http://eepurl.com/gTQThT

## Call for Articles

Call for Articles for 2021 Edition

We now invite original submissions for articles on any topic, and on all areas of law, relevant to the work of organisations from where ALIFDO has members, including any of ALIFDO's ten practice groups. A list of ALIFDO's Practice Groups can be found at www.alifdo.com/practice-groups

Reviews, case studies, alerts or any other material that may be of interest to ALIFDO members will also be considered.

If you would like to contribute, please contact us with your proposed article, or title and abstract for such article, by no later than 30 January 2021. Email: admin@alifdo.com. The complete article should then be sent to us by 30 April 2021.

All articles submitted should:

- be between 1000-10,000 words (longer articles may also be considered);
- be submitted in MS word format;
- acknowledge all sources;
- include your name, email address, employing organisation and city; and
- include a short abstract of between 150 and 300 words and up to ten keywords.

Materials will be published subject to ALIFDO's standard terms and conditions (see below).

For more information about this Journal please go to www.alifdo.com/alifdos-law-journal

**Terms and Conditions for publications in the Intergovernmental Organisations In-House Counsel Journal (IOICJ):**

1. Articles for inclusion in the IOICJ should be sent to admin@alifdo.com.
2. The article must be the original work of the author, should not have been previously published, and should not currently be under consideration by another journal. If it contains material which is someone else's copyright, the unrestricted permission of the copyright owner must be obtained and evidence of this submitted with the article and the material should be clearly identified and acknowledged within the text. The article shall not, to the best of the author's knowledge, contain anything which is libellous, illegal, or infringes anyone's copyright or other rights.
3. Copyright shall be assigned to ALIFDO and ALIFDO will have the exclusive right to first publication, both to reproduce and/or distribute an article (including the abstract) ourselves throughout the world in printed, electronic or any other medium, and to authorise others to do the same. Following first publication, such publishing rights shall be non-exclusive, except that publication in another journal will require permission from and acknowledgement of ALIFDO. Such permission may be obtained by contacting admin@alifdo.com.
4. Articles should follow the Intergovernmental Organisations In-house Counsel Journal's Style Guide, as found on ALIFDO's website (www.alifdo.com/alifdos-law-journal). Authors will be asked to sign a Publishing License.

# Contents

# Jurisdictional Immunity of International Organizations in the United States **in the Wake of the Supreme Court Decision in Jam v. IFC**

*Edward Chukwuemeke Okeke**

**Abstract:** The Supreme Court's decision in Jam v. International Finance Corporation has significantly altered the legal landscape of the jurisdictional immunity of international organizations in the United States. The Court held that under the International Organization Immunities Act (IOIA) international organizations are now entitled to the same "restrictive" immunity afforded foreign States under the Foreign Sovereign Immunities Act (FSIA). The decision has raised more questions than it answered. This article discusses how the IOIA came into being and has been construed up until the Jam decision. It analyzes the decision and its ramifications for those international organizations that derive their jurisdictional immunity in the United States from the IOIA.

## 1. Introduction

International organizations, which are different from non-governmental organizations or multinational corporations, are created by treaties or other international agreements by their member States to fulfill functions with which they have been entrusted. International organizations possess their own international personality and are subjects of international law.[1] The League of Nations which was established in 1920 following the Treaty of Versailles that ended World War I was the first modern international organization, but the United States was not a member of this forerunner of the United Nations. The dawn of contemporary international organizations was the end of the World War II, and the United States had championed their creation. The United States hosted the United Nations Monetary and Financial Conference, at Bretton Woods, New Hampshire, July 1-22, 1944 (the "Bretton Woods Conference"), which gave birth to both the International Monetary Fund and the International Bank for Reconstruction and Development. It also hosted the United Nations Conference on International Organization, in San Francisco, in June 1945 (the "San Francisco Conference"), which gave birth to the United Nations. As at now, the United States is involved in about 200 international organization and is the seat of about 20 of them.[2] Consequently, the position of the United States on the jurisdictional immunity of international organizations matters from both an international law and international cooperation perspective.

On February 27, 2019, the United States Supreme Court rendered its decision in *Jam v. International Finance Corporation*.[3] The decision has altered the legal landscape of the jurisdictional immunity of international organizations in the United States under the International Organizations Immunities Act (IOIA).[4] The Supreme Court held that the IOIA affords international organizations the same immunity from suit that foreign governments enjoy today under the

* Author, Jurisdictional Immunities of States and International Organizations (Oxford University Press 2018).

[1] *Reparation for Injuries Suffered in the Service of the United Nations*, Advisory Opinion, 1949 I.C.J. 174 (April 11).

[2] Brief for the United States as Amicus Curiae, Jam v. IFC, No. 17-1011.

[3] *Jam v. Int'l Fin. Corp.*, 139 S. Ct. 759 (2019).

[4] International Organizations Immunities Act of 1945 (IOIA or Act), Pub. L. No. 79-291, 59 Stat. 668 (22 U.S.S. 288, et seq).

Foreign Sovereign Immunities Act (FSIA).[5] To appreciate the ramifications of the decision, it is pertinent to understand the legal and legislative landscape for the jurisdictional immunity of international organizations before the Supreme Court weighed in with its own interpretation of the IOIA. In the end, the decision clarified the effect of the FSIA on the IOIA and settled the split between the Court of Appeals of the District of Columbia Circuit (D.C. Circuit) and the Court of Appeals of the Third Circuit (3rd Circuit) about the scope of immunity from suit of international organizations under the IOIA. The lower courts now have the task of applying the statutory framework and jurisprudence of the FSIA to international organizations that derive their immunity in the United States from the IOIA.

## 2. Legal and Legislative Landscape

International immunities evolve and diverge. Diplomatic privileges and immunities were the historical origins of the privileges and immunities of international organizations.[6] Article 7(4) of the Covenant of the League of Nations provided: "Representatives of the Members of the League and officials of the League when engaged on the business of the League shall enjoy diplomatic privileges and immunities." Similarly, Article 3 of the Headquarters Agreement of the International Labor Organization (ILO) provides that the organization "enjoys the immunities known in international law as diplomatic immunities." During the nascence of international organizations, it was a matter of convenience to analogize their immunities to those of diplomatic missions.[7] It was against this backdrop and international law landscape that the IOIA was enacted on December 29, 1945.

The impetus for the enactment of the IOIA was the Report of the Secretary of State to the President of the United States after the San Francisco Conference on the Charter of the United Nations. The Report noted that the operation of the provisions of Article 105 of the United Nations Charter may not be automatic and that as far "the United States is concerned, legislation will be needed to enable the officials of the United States to afford all of the appropriate privileges and immunities due the Organization and its officials under this provision."[8] The Report also noted:

> The United Nations, being an organization of all of the member states, is clearly not subject to the jurisdiction or control of any one of them…. The problem will be particularly important in connection with the relationship between the United Nations and the country in which it has its seat…. The United States shares the interest of all Members in seeing that no state hampers the work of the Organization through the imposition of unnecessary local burdens…[9]
>
> Several United Nations conferences which have already been held and which have either established or proposed the establishment of international organizations, have made provision in one way or another for the privileges and immunities of the organizations and their officials. This has been true in regard to the conferences which dealt with the Food and Agriculture Organization, UNRRA, the International Monetary Fund, the International Bank for Reconstruction and Development, and the Provisional International Civil Aviation Organization.[10]

The basic purpose of the legislation "is to confer upon international organizations and officials and employees thereof, privileges and immunities of a governmental nature."[11] The Report of the House of Representative noted:

> [T]here exists at the present time no law of the United States whereby this country can extend privileges and immunities of a governmental character with respect to international organizations or their officials in this country. It is to fill this need that this bill has been presented. As was pointed out by the Department of State, the self-interest of this Government in legislation of this character is two-fold since such legislation will not only protect the official character of public international organizations located in this country but it will also tend to strengthen the position of international organizations of which the United States is a member when they are located or carry on activities in other countries.[12]

Enacting the legislation became urgent because of the "increased activities of the United States in relation to international organizations [and] the probability that the United Nations Organization may establish its headquarters in this country, and the practical certainty in any case that it would carry on certain activities in this country, makes it essential to adopt this type of legislation promptly."[13] The precedents for the legislation were the Modus Vivendi between the League of Nations and the Government of Switzerland, and the 1944 Diplomatic Privileges (Extension) Act by which the British Government extended privileges and immunities to international organizations.[14] Although the Covenant of the League of Nations did not provide for its jurisdictional immunity, Article 1 of the Modus Vivendi provided that the organization "cannot, in principle, according to the rules of international law,

[5] Foreign Sovereign Immunity Act of 1976 (FSIA), 28 U.S.C. 1602.

[6] Edward Chukwuemeke Okeke, Jurisdictional Immunities of States and International Organizations, at 348 (Oxford University Press 2018).

[7] Ibid., at 349.

[8] 1 Charter of the United Nations. Report to the President on the Results of the San Francisco Conference by the Chairman of the United States Delegation, the Secretary of State, June 26, 1945, Department of State Publication 2349, Conference Series 71, at 160.

[9] Ibid., at 159.

[10] Ibid.

[11] Committee on Ways and Means, Granting Certain Privileges and Immunities to International Organizations and their Employees, H.R. Rep. No. 1203, 79th Cong., 1st Sess. 1 (1945), at 1.

[12] Ibid., at 2.

[13] Ibid.

[14] Ibid., at 3.

be sued before the Swiss Courts without its express consent."[15] In the same vein, the United Kingdom Diplomatic Privileges (Extension) Act provided "Immunity from suit and legal process" for international organizations.[16]

In 1945 Congress enacted the IOIA which defines an "international organization" as:

> [A] public international organization in which the United States participates pursuant to any treaty or under the authority of any Act of Congress authorizing such participation or making an appropriation for such participation, and which shall have been designated by the President through appropriate Executive order as being entitled to enjoy the privileges, exemptions, and immunities provided in this [Act].

The IOIA authorizes the President:

> [I]n the light of the functions performed by any such international organization, by appropriate Executive order to withhold or withdraw from any such organization or its officers or employees any of the privileges, exemptions, and immunities provided for in this [Act] (including the amendments made by this [Act]) or to condition or limit the enjoyment by any such organization or its officers or employees of any such privilege, exemption, or immunity.

The IOIA also authorizes the President:

> [I]f in his judgment such action should be justified by reason of the abuse by an international organization or its officers and employees of the privileges, exemptions, and immunities provided in this subchapter or for any other reason, at any time to revoke the designation of any international organization under this section, whereupon the international organization in question shall cease to be classed as an international organization for the purpose of this [Act].

Section 2 (a) of the IOIA provides pertinently:

> International organizations, their property and their assets, wherever located, and by whomsoever held, shall enjoy the same immunity from suit and every form of judicial process as is enjoyed by foreign governments, except to the extent that such organizations may expressly waive their immunity for the purpose of any proceedings or by the terms of any contract.[17]

When the IOIA was enacted, the United States applied the doctrine of absolute sovereign or State immunity, under which a foreign State cannot be sued in the court of another sovereign without its consent.[18] However, in 1952, the State Department through the famous Tate letter declared its adoption of the doctrine of restrictive sovereign or State immunity, under which foreign States are generally immune only for their sovereign or public acts (*acta jus imperii*), but not for their commercial or private acts (*acta jure gestionis*).[19] The letter stated inter alia:

> Furthermore, the granting of sovereign immunity to foreign governments in the courts of the United States is most inconsistent with the action of the Government of the United States in subjecting itself to suit in these same courts in both contract and tort and with its long established policy of not claiming immunity in foreign jurisdictions for its merchant vessels. Finally, the Department feels that the widespread and increasing practice on the part of governments of engaging in commercial activities makes necessary a practice which will enable persons doing business with them to have their rights determined in the courts. For these reasons it will hereafter be the Department's policy to follow the restrictive theory of sovereign immunity in the consideration of requests of foreign governments for a grant of sovereign immunity.[20]

In 1976, Congress enacted the Foreign Sovereign Immunities Act (FSIA) which codified the doctrine of restrictive sovereign immunity.[21] Under the FSIA, foreign States, their agencies and instrumentalities are immune from suit unless the claim falls within the enumerated exceptions under the statute.[22] The exceptions permit, inter alia, certain actions against a foreign State that arise out of its commercial activities with the requisite territorial nexus to the United States,[23] territorial or noncommercial torts committed in the United States,[24] or rights in immovable property in the United States.[25] The primary purposes of the FSIA are to codify the doctrine of restrictive sovereign immunity and to shift the determination of immunity of foreign States from the State Department to the courts.

The debate had raged as to whether the FSIA altered the scope of immunity of international organizations under the IOIA, with commentators and courts alike weighing in, before the Supreme Court decided the question.

---

[15] 7 League of Nations O.J. 1422 (1926).

[16] Diplomatic Privileges (Extension) Act, 1944, 7 & 8 Geo 6, chapter 44, Section 1, Schedule 1

[17] *22 U.S.C. § 288a*.

[18] See, *Republic of Austria v. Altmann*, 541 U.S. 677, 690 (2004).

[19] See, Letter from Jack B. Tate, Acting Legal Adviser, U.S. Dep't of State to Philip B. Perlman, Acting Attorney General (May 19, 1952), *reprinted in, Alfred Dunhill of London, Inc. v. Republic of Cuba*, 425 U.S. 682, 711-714 (1976) and in 26 Dep't State Bull. 984 (1952).

[20] 425 U.S. at 714.

[21] 28 U.S.C. 1602 *et seq.*

[22] 28 U.S.C. 1604; see *Verlinden B.V. v. Central Bank of Nigeria,* 461 U.S. 480, 488 (1983).

[23] 28 U.S.C. 1605(a)(2); see, *OBB Personenverkehr AG v. Sachs*, 136 S. Ct. 390 (2015).

[24] 28 U.S.C. 1605(a)(5); see, *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428, 441 (1989).

[25] 22 U.S.C. 1605(a)(4); see *Permanent Mission of India to the U.N. v. City of N.Y.*, 551 U.S. 193, 196-7 (2007).

## 3. Analysis of the Jam Decision

In *Jam*, the following questions were presented in the Petition for a Writ of Certiorari to the United States Court of Appeals for the D.C. Circuit:

1. Whether the International Organizations Immunities Act—which affords international organizations the "same immunity" from suit that foreign governments have, 22 U.S.C. § 288a(b)—confers the same immunity on such organizations as foreign governments have under the Foreign Sovereign Immunities Act, 28 U.S.C. §§ 1602-11.

2. If not, what are the rules governing the immunity to which international organizations are entitled?

The United States Supreme Court granted certiorari limited to only Question 1.

The defendant, International Finance Corporation (IFC), an international organization headquartered in the United States, had provided loans to an Indian company to co-finance the construction and operation of a coal-fired power plant in India. In accordance with IFC's policy to prevent environmental and social damage, the loan agreement included an Environmental and Social Action Plan designed to protect surrounding communities at the power plant from such damage. The IFC Compliance Advisor Ombudsman (CAO) conducted an internal audit which concluded that the construction and operation of the plant did not comply with the Plan.

The plaintiffs, represented by EarthRights International, a nongovernmental organization (NGO), are Indian fishermen, farmers, a local government entity, and a trade union of fishermen who claim that their way of life has been devastated. Relying on the report of the CAO, the plaintiffs base their claims on various torts. They also assert a breach of contract, claiming to be third party beneficiaries of the environmental and social terms of the loan agreement. They argued that IFC is not immune to their claims and even if it was immune, it has waived the immunity under its Articles of Agreement. The District Court of the District of Columbia (D.C.) dismissed their claims based on the D.C. Circuit precedent that the IOIA granted international organizations absolute immunity as enjoyed by foreign States when the IOIA was enacted.[26] The Court of Appeals for the D.C. Circuit affirmed and agreed with the District Court that IFC was immune under the IOIA based on its precedent.[27] However, in a concurring opinion that read more like a dissent, Judge Pillard observed that if she were not bound by precedent she would have construed the IOIA differently and along the lines of the interpretation of the Third Circuit in *OSS Nokalva v. European Space Agency*, 617 F.3d 756 (3d Cir. 2010).[28] The case was appealed to the Supreme Court.

The narrow issue before the Supreme Court did not involve an interpretation of the Articles of Agreement of the IFC. As stated by the Supreme Court itself, "this cases requires us to determine whether the IOIA grants international organizations the virtually absolute immunity foreign governments enjoyed when the IOIA was enacted, or the more limited immunity they enjoy today.[29] In a 7–1 majority decision delivered by Chief Justice John Roberts, the Supreme held:

> The International Organizations Immunities Act grants international organizations the "same immunity" from suit "as is enjoyed by foreign governments" at any given time. Today, that means that the Foreign Sovereign Immunities Act governs the immunity of international organizations. The International Finance Corporation is therefore not absolutely immune from suit.[30]

The decision of the Supreme Court overturned the judgment of the D.C. Circuit Court of Appeals in the case and the longstanding jurisprudence of Atkinson v. Inter-American Development Bank. The majority opinion had taken a very textualist approach to statutory interpretation:

> In granting international organizations the "same immunity" from suit "as is enjoyed by foreign governments," the Act seems to continuously link the immunity of international organizations to that of foreign governments, so as to ensure ongoing parity between the two. The statute could otherwise have simply stated that international organizations "shall enjoy absolute immunity from suit," or specified some other fixed level of immunity. Other provisions of the IOIA, such as the one making the property and assets of international organizations "immune from search," use such non-comparative language to define immunities in a static way. 22 U. S. C. §288a(c). Or the statute could have specified that it was incorporating the law of foreign sovereign immunity as it existed on a particular date.[31]

The Supreme Court construed the "same as" formulation in the IOIA to mean that the immunity of international organizations and that of foreign sovereign are continuously equivalent. It applied the "reference" canon of statutory interpretation and concluded that "when a statute refers to a general subject, the statute adopts the law on that subject as it exists whenever a question under the statute arises."[32]

---

[26] See, 172 F. Supp. 3d 104, 108-9 (D.C. 2016) ) citing *Atkinson v. Inter-American Development Bank*, 156 F. 3d 1335 (D.C. Cir. 1998) where the Court of Appeals had decided that international organizations still had virtually absolute immunity as foreign States had when the IOIA was enacted in 1945.

[27] See 860 F.3d 703 (D.C. Cir. 2017).

[28] The Third Circuit in *Nokalva* declined to follow *Atkinson* and held that the doctrine of restrictive sovereign immunity as codified in the FSIA now applies to international organizations under the IOIA.

[29] Jam v. IFC, 139 S. Ct. 759, 765 (2019).

[30] 139 S. Ct at 772. Justice Steven Breyer was the lone dissent. Justice Kavanaugh who was new to the Supreme Court and was part of the *en banc* panel of the D.C. Circuit Court of Appeals that rejected reconsideration of the *Jam* case.

[31] Ibid., at 768.

[32] Ibid., at 769.

The Court continued:

> The IOIA's reference to the immunity enjoyed by foreign governments is a general rather than specific reference. The reference is to an external body of potentially evolving law—the law of foreign sovereign immunity—not to a specific provision of another statute. The IOIA should therefore be understood to link the law of international organization immunity to the law of foreign sovereign immunity, so that the one develops in tandem with the other.[33]

The Supreme Court held:

> The International Organizations Immunities Act grants international organizations the "same immunity" from suit "as is enjoyed by foreign governments" at any given time. Today, that means that the Foreign Sovereign Immunities Act governs the immunity of international organizations. The International Finance Corporation is therefore not absolutely immune from suit.[34]

The dissent by Justice Breyer did not think that the statutory language is as clear as the majority made it out to be. He concluded that the statute granted international organisations the same immunity that foreign states had in 1945 when the statute was enacted. To reach the conclusion, he relied on the "statute's history, its context, its purposes, and its consequences" in his conviction that "purpose-based methods of interpretation can often shine a useful light upon opaque statutory language, leading to a result that reflects greater legal coherence and is, as a practical matter, more sound."[35] He did not think that the temporal problem posed by the phrase "as is enjoyed" is resolvable by the reference canon because it is ultimately a matter of legislative intent and purpose: "Thus, all interpretation roads here lead us to the same place, namely, to context, to history, to purpose, and to consequences. Language alone cannot resolve the statute's linguistic ambiguity."[36] He concluded: "Given the differences between international organizations and nation states, along with the Act's purposes and the risk of untoward consequences, I would leave the Immunities Act where we found it—as providing for immunity in both commercial and noncommercial suits."[37]

## 4. Ramifications of the Jam Decision

The most important or consequential passage in the Supreme Court decision from an international law perspective is the following:

> To begin, the privileges and immunities accorded by the IOIA are only default rules. If the work of a given international organization would be impaired by restrictive immunity, the organization's charter can always specify a different level of immunity. The charters of many international organizations do just that. See, e.g., Convention on Privileges and Immunities of the United Nations, Art. II, §2, Feb. 13, 1946,21 U. S. T. 1422, T. I. A. S. No. 6900 ("The United Nations . . . shall enjoy immunity from every form of legal process except insofar as in any particular case it has expressly waived its immunity"); Articles of Agreement of the International Monetary Fund, Art. IX, §3, Dec. 27, 1945, 60Stat. 1413, T. I. A. S. No. 1501 (IMF enjoys "immunity from every form of judicial process except to the extent that it expressly waives its immunity"). Notably, the IFC's own charter does not state that the IFC is absolutely immune from suit.[38]

In the above passage the Supreme Court reconciled the IOIA with treaty law by making clear that IOIA is only a default rule and does not detract from the international law obligation under any applicable treaty. The *Jam* decision underscores that the primary source of the immunity from legal process for international organizations is their respective constituent instruments. The IOIA as a default rule would only apply or prevail in the absence of conflicting or more specific rules in an international agreement or treaty to which the United States is party.

Section 1 of the IOIA authorizes the U.S. President through appropriate Executive Order to designate international organizations that are entitled to enjoy certain privileges and immunities under the Act. To that effect, President Truman by Executive Order 9751 designated the International Bank for Reconstruction and Development (IBRD or World Bank) and the International Monetary Fund (IMF of Fund)), and stated pertinently that their designation,

> as public international organizations within the meaning of the said International Organizations Immunities Act is not intended to abridge in any respect privileges and immunities which such organizations have acquired or may acquire by treaty or Congressional action; **provided, that with respect to the International Bank for Reconstruction and Development, such designation shall not be construed to affect in any way the applicability of the provisions of section 3, Article VII, of the Articles of Agreement of the Bank** [emphasis added] as adopted by the Congress of the United States in the Bretton-Woods Agreements Act of July 31, 1945 (Public Law 171, 79th Congress).

Similarly, Executive Order 10680 by President Eisenhower stated:

> The designation of the International Finance Corporation made by this order is not intended to abridge in any respect privileges, exemptions, and immunities which such corporation may have acquired or may acquire by

[33] Ibid.

[34] Ibid., at 772.

[35] Ibid., at 773.

[36] Ibid., at 775.

[37] Ibid., at 781.

[38] Ibid., at 771.

treaty or Congressional action; **nor shall such designation be construed to affect in any way the applicability of the provisions of section 3, Article VI, of the Articles of Agreement of the Corporation** [emphasis added] deposited in the archives of the International Bank for Reconstruction and Development.

The import of these Executive Orders is that the ultimate determination of the scope of their jurisdictional immunity would entail an interpretation of their constituent instruments' provisions. Consequently, the question arises as to why the jurisdictional immunity of IFC had been examined under the IOIA considering the provision of Execution Order 10680.[39] The answer may lie in the ambiguity of the text of Article VI, Section 3, of the IFC Articles of Agreement. A judicial review and application of the IOIA as the rule of decision, to the exclusion of international law, i.e., relevant treaty, could invite lower courts to ignore such treaty obligations, and to engage in an exclusive and ultimately unproductive analysis under only the IOIA. The scope of immunity depends on the source of the immunity.

Even though the Supreme Court determined that international organizations that derive their jurisdictional immunity in the United States from the IOIA are now subject to restrictive immunity as codified in FSIA, it is not the end of the analysis. Congress enacted the IOIA in 1945, ratified the IFC Articles in 1956, and enacted the FSIA in 1976. The FSIA may not be applicable to some international organizations because of the treaty exclusion under §1604 (Immunity of a foreign state from jurisdiction) of the FSIA: "Subject to existing international agreements to which the United States is a party at the time of enactment of this Act a foreign state shall be immune from the jurisdiction of the courts of the United States and of the States except as provided in sections 1605 to 1607 of this chapter." Thus, under the treaty exclusion to the FSIA exceptions, the determination of the scope of immunity of some international organizations would lead back to their constituent instruments or treaties to which the United States is a party. Also, under the so-called later-in-time rule, a treaty that has been incorporated into United States law would also prevail over the IOIA/FSIA default rules.[40] A treaty has domestic effect if it is self-executing or there is an implementing legislation by Congress.[41] The treaty exclusion would preserve the international law obligation of the United States.

Where the United States is a member of an international organization and party to any convention or treaty on the immunity of that organization, the IOIA must be construed to be in harmony with the international legal instrument.[42] Moreover, Supreme Court had exhorted courts to construe federal statutes, wherever possible, as not to violate international law, in what is known as the *Charming Betsy* canon from the eponymous case.[43] The Supreme Court has also held that "a treaty will not be deemed to have been abrogated or modified by a later statute unless such purpose on the part of Congress has been clearly expressed."[44] The sources of the law are very critical to the determination of the scope of jurisdictional immunity of international organizations, which may revolve around the interpretation of international or national law or both, and should be construed in *pari materia*, as applicable.

The Supreme Court had eschewed any discussion of the nature and purpose of the immunity of international organizations vis-à-vis that of foreign States. It had decided that the FSIA standards will be applied to the IOIA, without construing the FSIA to determine whether Congress intended the FSIA to apply to international organizations. The problem with assimilating or incorporating the FSIA into the IOIA for the determination of the scope of immunity of international organizations revolves around the restrictive sovereign immunity distinction between sovereign acts and private or commercial acts, considering that international organizations do not undertake sovereign acts but acts in the exercise of their functions. It is not farfetched that acts performed in fulfilment of the functions of an international organization would be private or commercial acts if undertaken by a foreign State.

To the concern that applying the doctrine of restrictive sovereign immunity to international development banks would yield undesirable results because these international organizations "use the tools of commerce to achieve their objectives," they may be subject to suit under the FSIA's commercial activity exception for most or all of their core activities, unlike foreign sovereigns, the Supreme Court noted:

> Nor is there good reason to think that restrictive immunity would expose international development banks to excessive liability. As an initial matter, it is not clear that the lending activity of all development banks qualifies as commercial activity within the meaning of the FSIA. […] As the Government suggested at oral argument, the lending activity of at least some development banks, such as those that make conditional loans to governments, may not qualify as "commercial" under the FSIA.[45]

The Supreme Court continued:

> And even if an international development bank's lending activity does qualify as commercial, that does not mean the organization is automatically subject to suit. The FSIA includes other requirements that must also be met. For one thing, the commercial activity must have a sufficient nexus to the United States. See 28 U.

[39] 3 CFR 86 (1957); 22 U.S.C. §§282, 288.

[40] See, e.g., *Whitney v. Robertson*, 124 U.S. 190, 195 (1888).

[41] See, *Medellin v. Texas*, 552 U.S. 491, 505 (2008).

[42] See *Brzak v. United Nations*, 597 F.3d 107, 112 (2d Cir. 2010) (declining to determine the scope of immunity of the United Nations under the IOIA because the Convention on the Privileges and Immunities of the United Nations to which the United States acceded in 1970 granted the absolute immunity to the United Nations).

[43] See *Alexander Murray v. Schooner Charming Betsy*, 4 U.S. 64 (1804).

[44] See *Trans World Airlines Inc. v. Franklin Mint Corp.*, 466 U.S. 243, 251– 52 (1984) citing Cook v. United States, 288 U.S. 102, 120 (1933).

[45] 139 S. Ct. at 772.

> S. C. §§1603, 1605(a)(2). For another, a lawsuit must be "based upon" either the commercial activity itself or acts performed in connection with the commercial activity. See §1605(a)(2). Thus, if the "gravamen" of a lawsuit is tortious activity abroad, the suit is not "based upon" commercial activity within the meaning of the FSIA's commercial activity exception. See OBB Personenverkeh r AG v. Sachs, 577 U. S. ___, ___–___ (2015); Saudi Arabia v. Nelson, 507 U. S. 349, 356–359 (1993). At oral argument in this case, the Government stated that it has "serious doubts" whether petitioners' suit, which largely concerns allegedly tortious conduct in India, would satisfy the "based upon" requirement. Tr. of Oral Arg. 25–26. In short, restrictive immunity hardly means unlimited exposure to suit for international organizations.[46]

The dictum is cold comfort for international organizations that derive their immunity from the IOIA as they may face increased litigation as lower courts sort out this new standard. The commercial activity exception depends on the nature of the activity, as opposed to the purpose. According to the drafting history of the FSIA, "the fact that goods or services to be procured through a contract are to be used for a public purpose is irrelevant; it is the essentially commercial nature of an activity or transaction that is critical."[47]

However, purpose is key under the "functional necessity" principle in the determination of the immunity of international organizations. Another problem for international organizations with the commercial activity exception is that the exception subsumes employment contracts. The House Report on the FSIA includes in the definition of commercial activity "sale of a service or a product, its leasing of property, its borrowing of money, its employment or engagement of laborers, clerical staff or public relations or marketing agents."[48] It also states that "public or governmental and not commercial in nature, would be the employment of diplomatic, civil service, or military personnel, but not the employment of American citizens or third country nationals by the foreign state in the United States."[49] Hopefully, the employment of international civil servants by international organizations would be analogized to members of the diplomatic and civil service of foreign states, which would avoid the problem with the adjudication of employment disputes by U.S. courts:

> An attempt by the courts of one nation to adjudicate the personnel claims of international civil servants would entangle those courts in the internal administration of those organizations. Denial of immunity opens the door to divided decisions of the courts of different member states passing judgment on the rules, regulations, and decisions of the international bodies. Undercutting uniformity in the application of staff rules or regulations would undermine the ability of the organization to function effectively.[50]

## 5. Conclusion

The *Jam* decision does not and should not alter the treaty obligation of the United States to accord certain international organizations the so-called absolute immunity under their respective constituent instruments. By recognizing and ruling that the primary source of the immunity from suit of international organizations is their constituent instrument and that the IOIA is but a default rule, the *Jam* decision has appropriately reconciled the national law with international law. This reconciliation, however, leaves unresolved for now how the immunity from suit of international organizations under the IOIA would fit into the statutory scheme of the entire FSIA, with all its enumerated exceptions, and its procedures, which was evidently enacted without international organizations in mind. This is the challenge for the lower courts.

[46] Ibid., at 772.

[47] H.R. REP. 94-1487, 16 (1976).

[48] Ibid.

[49] Ibid., at 16.

[50] *Broadbent v. OAS*, 628 F.2d 27, 34-5 (D.C. Cir. 1980).

# Treatment of Corporate Groups **under Multilateral Development Banks' Sanctions Regimes**

*Jelena Madir**

**Abstract:** In 2010, the heads of five leading multilateral development banks (MDBs) – the African Development Bank, the Asian Development Bank, the European Bank for Reconstruction and Development, the Inter-American Development Bank and the World Bank Group – signed the Agreement for Mutual Enforcement of Debarment Decisions, which provides for mutual and reciprocal enforcement of debarment decisions taken by any one of the MDBs against parties that engage in fraud, corruption, coercion and collusion in connection with MDB-financed projects. For parties that are seeking financing form an MDB or are competing for contracts funded by an MDB, this means that a sanctionable practice committed in a single country could result in global sanctions. Sanctions procedures of each individual MDB provide that sanctions may be applied to the affiliates and successors of sanctioned parties. Nevertheless, a number of challenging issues surround the need to, on the one hand, prevent the circumvention of MDBs' sanctions through the use of affiliates or changes in corporate forms and, on the other hand, ensure that sanctions are commensurate with the degree of responsibility, especially where a sanctioned party has numerous affiliates operating in different business sectors around the globe. In order to provide guidance on these matters, in 2012, the MDBs adopted the Harmonised Principles on Treatment of Corporate Groups, which set out general guidance on the application of sanctions to affiliates and successors. While the Principles provide a useful starting point, they would benefit from further guidance in order to facilitate clearer standards for the MDBs. To that end, this article analyses four main areas of corporate liability: (i) liability of a company for its employees' wrongdoings, (ii) liability of a parent company for its subsidiaries' wrongdoings, (iii) liability of a subsidiary for its parent company's wrongdoings and (iv) successor liability, and proposes recommendations for further guidance under the Principles.

## 1. Introduction

In April 2010, the heads of five leading multilateral development banks ("MDBs" and each, an "MDB")–the African Development Bank, the Asian Development Bank, the European Bank for Reconstruction and Development (EBRD), the Inter-American Development Bank and the World Bank Group (WB)–signed the Agreement for Mutual Enforcement of Debarment Decisions (the "Cross-Debarment Agreement"), which provides for mutual and reciprocal enforcement of debarment decisions taken by any one of them against parties that engage in fraud, corruption, coercion or collusion (each, a "sanctionable practice") in connection with MDB-financed projects. For parties that are seeking financing form an MDB or are competing for contracts funded by an MDB, this means that a sanctionable practice committed in a single country could result in global sanctions.

All MDBs' sanctions procedures state that affiliates of respondents may also be sanctioned and that sanctions may

* General Counsel, Gavi, the Vaccine Alliance. I would like to thank Chiawen Kiew, Associate Director at the European Bank for Reconstruction and Development, for his comments on this article.

be applied to successors and assigns of sanctioned parties. Nevertheless, a number of challenging issues surround the need to prevent the circumvention of the MDBs' sanctions through the use of affiliates or changes in corporate forms, on the one hand, while on the other hand ensuring that sanctions are commensurate with the degree of responsibility, especially where a sanctioned party has numerous affiliates operating in different business sectors around the globe. In order to provide guidance on these matters, in September 2012, the MDBs adopted the Harmonised Principles on Treatment of Corporate Groups (the "Principles"), which set out general principles for the application of sanctions to affiliates and successors and assigns.[1]

While the Principles provide a useful starting point, they would benefit from further guidance in order to facilitate clearer standards for the MDBs. For example, the Principles recommend that sanctions should be applied to the sanctioned party's parent company if that company was involved in the sanctionable practice. Such involvement may include wilful blindness and failure to supervise. However, without sufficient guidance on this issue, the "failure to supervise" standard may allow a company to successfully argue that it had properly supervised its employees, but that its employees acted "rogue" in committing a sanctionable practice. Similarly, without more detailed standards to address successor liability, companies could evade sanctions by dissolving and taking on another legal form.

This article makes recommendations for further guidance under the Principles, based on the analysis of the laws of the United States (US) and the United Kingdom (UK). The choice of the US and the UK as benchmark jurisdictions was guided by two factors: (i) first, the fact that MDBs' sanctions regimes are based on the US Federal Acquisition Regulation (FAR)[2] and thus founded on common law principles and (ii) second, the fact that three out of the five MDBs are headquartered in these two jurisdictions. After an overview of the Principles in Section 2, the subsequent Sections analyse four main areas of corporate liability: (i) liability of a company for its employees' wrongdoings, (ii) liability of a parent company for its subsidiaries' wrongdoings, (iii) liability of a subsidiary for its parent company's wrongdoings and (iv) successor liability. Each Section concludes the analysis by making recommendations for further enhancements of and clarifications under, the Principles.

## 2. Overview of the Principles

The Principles recognise that sanctions should be applied to entities within corporate groups, based on the facts of the relevant case and not a rigidly automatic approach. Nevertheless, the Principles state a rebuttable presumption that sanctions should be applied to all entities **controlled by** the respondent, unless the respondent demonstrates that the entities are free of responsibility for the misconduct, application to the entities would be disproportional and is not reasonably necessary to prevent evasion.[3] In practice, however, very few respondents focus on the possibility that their subsidiaries may be captured by the sanction and hence fail to rebut this presumption in their response to the allegations of sanctionable practices, which then by default results in the sanctions typically extending to affiliates controlled by the sanctioned parties.

The Principles additionally recommend that sanctions be applied to entities **controlling** the respondent and to entities under common control, if the relevant entity was involved in the sanctioned misconduct.[4] Such involvement may include wilful blindness and failure to supervise.[5] The WB Sanctions Board's stance has been to impose a sanction based on a finding of either (i) culpability for direct involvement (e.g., through instructions or orders, approval or guidance, or inferred authorisation in cases of close supervision),[6] or (ii) responsibility for another party's actions (e.g., where there is a duty to supervise combined with deliberate non-intervention).[7] Needless to say, it is challenging as a practical matter to establish that a parent company had a duty to supervise the subsidiary found to have engaged in a sanctionable practice. In addition, critics have suggested that concepts such as wilful blindness and failure to supervise should be applied sparingly and that the MDBs' sanctions determinations should respect the doctrine of corporate separateness, which is observed in civil and common law systems worldwide.[8]

Furthermore, the Principles recommend that the sanction should be applied to the successor or assign of a sanctioned party, unless the successor or assign demonstrates that such application would be unreasonable.[9] Moreover, the Principles also state that "the business operations of the originally sanctioned entity should continue to be sanctioned".[10] It is unclear how a sanction can apply to "business operations", given that business operations of an entity are not legal entities themselves.

Additionally, the Principles recommend that, if a *prima facie* case has been made that an individual who is subject

[1] MDB Harmonized Principles on Treatment of Corporate Groups (10 September 2012), available at: http://lnadbg4.adb.org/oai001p.nsf/0/A7912C61C52A85AD48257ACC002DB7EE/$FILE/MDB%20Harmonized%20Principles%20on%20Treatment%20of%20Corporate%20Groups.pdf [hereinafter the "Principles"].

[2] The US Federal Acquisition Regulation served as the basis for the World Bank Group's Sanctions Procedures, which in turn served as the basis for the sanctions procedures of the other four MDBs.

[3] The Principles, A.3.

[4] Ibid., A.4.

[5] Ibid.

[6] See, e.g., World Bank Sanctions Board Decision No. 65 (2014), ¶59 and Sanctions Board Decision No. 49 (2012), ¶¶19-31 (applying a sanction to an affiliate under common control with the respondent where the affiliate was found to have been directly involved in the misconduct).

[7] See, e.g., World Bank Sanctions Board Decision No. 65 (2014), ¶59.

[8] Freshfields Brockhaus Deringer US LLP, *Submission of Freshfields Brockhaus Deringer LLP in connection with Review of the World Bank Group Sanctions System* (2013), at 13.

[9] The Principles, A.5.

[10] Ibid.

to a sanction has been employed or engaged by an entity, then the MDBs may apply the sanction to the employing or engaging entity if the individual was engaged to evade a sanction.[11] Clearly, this principle is intended to prevent sanctioned individuals from evading a sanction by working on a project on which their company is working with an MDB. For example, the WB Sanctions Board has typically held that an employer could be found liable for the acts of its employees under the doctrine of *respondeat superior*, considering in particular whether the employees acted within the scope of their employment and were motivated, at least in part, by the intent of serving their employer. Where a respondent entity has denied responsibility for the acts of its employees based on a rogue employee defence, the Sanctions Board has assessed any evidence presented regarding the scope and adequacy of the respondent entity's controls and supervision at the time of the misconduct.[12]

Lastly, with respect to cross-debarments, the Principles state that only such sanctioned entities within a corporate group that are identified by name by the sanctioning institution are subject to cross-debarment pursuant to the Cross-Debarment Agreement.[13] This approach is understandable, because if the debarment applied to the respondent and "all of its affiliates" or "all of the affiliates controlled by the respondent", without identifying such affiliates by name, it would be impossible to know which companies were captured by the cross-debarment without undertaking a thorough analysis of the organisational structure of a company attempting to work on an MDB-financed project. This would be impractical in view of the hundreds of debarred companies on the list. On the other hand, if the debarment were to apply only to the specifically named affiliates, this would generate the risk that a debarred party may simply create a new affiliate with a name different from any of the names on the list and consequently avoid debarment. EBRD's sanctions procedures (the Enforcement Policy and Procedures) attempt to deal with such risk by placing the onus of detecting circumvention attempts on the Office of the Chief Compliance Officer (OCCO) by stating that if, after the issuance of the first-tier decision-maker's decision or the final decision by the appellate body (the Enforcement Committee), OCCO determines prima facie that an entity that is seeking to get funding (directly or indirectly) from an EBRD-financed project (the "New Entity") is a successor or assignee of sanctioned entity, including through the acquisition of or merger with that entity, OCCO may apply to the first-tier decision-maker to have the original sanction applied to the New Entity.[14]

## 3. Liability of a company for its employees' wrongdoings

The basic feature of corporate personality is that the corporation is a legal entity distinct from its shareholders. The main advantage that a company has is that it is capable of having rights and being subject to duties which are not identical as those enjoyed or borne by its shareholders. It has distinct legal personality from any individual person and thus longevity beyond that of its members. Nonetheless, there are instances when the law makes companies vicariously liable for their employees' wrongdoings. After all, one could argue that, given that the company has no mind of its own, in order to evaluate the company's acts, it is necessary to refer to the acts of its employees. This Section analyses the liability of a company for its employees' wrongdoing under the US and UK law, and makes suggestions for enhancements of the Principles.

### 3.1. US law

In the US, under the doctrine of *respondeat superior*, a company may be held criminally liable for the illegal acts of its directors, officers, employees and agents. To hold a company liable for these actions, the government must establish that the company agent's actions (i) were within the scope of his duties and (ii) were intended, at least in part, to benefit the company.[15]

As for the first element, an employee is considered to be acting within the scope of his/her duties if (s)he has actual or apparent authority to engage in the act in question.[16] Moreover, an employee is acting with apparent authority if a third party reasonably believes that (s)he has the authority to perform the act in question.[17]

As to the second element, as established in *Automated Medical Laboratories*, the company does not necessarily need to profit from its agent's actions for it to be held liable. In that context, the US Court of Appeals for the 4th Circuit stated:

> Benefit is not a 'touchstone of criminal corporate liability; benefit at best is an evidential, not an operative fact.' Thus, whether the agent's actions ultimately [accrued] to the benefit of the corporation is less significant than whether the agent acted with the intent to benefit the corporation. The basic purpose of requiring that an agent have acted with the intent to benefit the corporation, however, is to insulate the corporation from criminal liability for actions of its agents which may be inimical to the interests of the corporation or which may have been undertaken solely to advance the interests of that agent or of a party other than the corporation.[18]

[11] Ibid., C.2(b).

[12] World Bank Sanctions Decision No. 83 (30 September 2015), ¶69.

[13] The Principles, D.1.

[14] EBRD's *Enforcement Policy and Procedures* (2017), §11.2(i).

[15] Offices of the United States Attorneys, *Principles of Federal Prosecution of Business Organizations*, §9-28.010.

[16] See, e.g., *A.I. Credit Corp v Legion Ins. Co.*, 265 F.3d 630 (7th Cir. 2001), at 637 and *Zurich Capital Mkts. v Coglianese*, 332 F. Supp. 2d 1087 (N.D. Ill. 2004), at 1108.

[17] See, e.g., *United States v Bi-Co Pavers, Inc.*, 741 F.2d 730 (5th Cir. 1984), at 737.

[18] *United States v Automated Medical Laboratories Inc*. 770 F. 2d 399, at 407 (4th Cir. 1985).

Companies can be held liable for crimes committed by low-level employees,[19] contrary to corporate directives,[20] or notwithstanding the company's adoption of an effective compliance programme, although–as further described below–a company that had an effective compliance programme, self-reported and cooperated is eligible for a reduced fine.[21] In addition, under the wilful blindness doctrine, a company can be held criminally liable for deliberately disregarding the criminal activity at hand.[22] Therefore, if a company should have known of a wrongdoing, it should not recklessly fail to address it.

Notably, in the recent years, the emphasis has been on seeking accountability from the individuals who perpetrated the wrongdoing. In that context, in September 2015, Sally Yates, the then Deputy Attorney General of the Department of Justice, issued the Memorandum on Individual Accountability for Corporate Wrongdoers (the "Yates Memo"), which signals that the Department of Justice (DOJ) would proceed more aggressively in targeting individuals involved in corporate wrongdoing, emphasising that "one of the most effective ways to combat corporate misconduct is by seeking accountability from the individuals who perpetrated the wrongdoing". This is because "such accountability [...] deters future illegal activity, it incentivizes change in corporate behaviour, it ensures that proper parties are held responsible for their actions and it promotes the public's confidence in the justice system".[23]

The Yates Memo was likely issued in response to widespread criticism that, following the 2008 financial crisis, the DOJ pursued enforcement actions against financial institutions without a successful prosecution of any senior officers employed by those organisations.[24] The Memo has raised concerns that lower-level personnel may feel pressured to provide government investigators with what they want as opposed to facts that might be less helpful to investigators and that higher-level officials will be less cooperative due to fears of potential individual liability.[25] In response to this criticism, in November 2018, the Deputy Attorney General, Rod Rosenstein, announced that, in contrast to the requirements in the Yates Memo, a corporation now need not identify every individual who might face civil liability in order to receive maximum cooperation credit in civil cases, but rather only those individuals who were "substantially involved in" or "responsible for" the alleged misconduct.[26] However, the DOJ will not award any credit to a corporation that "conceals involvement in the misconduct by members of senior management or the board of directors" or that "otherwise demonstrates a lack of good faith in its representations regarding the nature or scope of the misconduct".[27]

Importantly for MDBs' sanctions procedures, under the Foreign Corrupt Practices Act (FCPA), a company is vicariously liable when its directors, officers, employees or agents, acting within the scope of their employment, commit FCPA violations intended, at least in part, to benefit the company.[28] As there is no requirement for the culpable employee to be of a certain seniority, it is relatively easy for the prosecution to discharge its burden of proof regarding the company's liability.[29] For criminal liability to apply to a company, there must be corporate "knowledge"–either through individual corporate employees or through the doctrine of "collective knowledge", which imputes to a company the sum knowledge of all or some of its employees by aggregating individual employee's knowledge for the purpose of creating the necessary guilty intent for the corporation. Thus, a company may be liable even if there is no single employee entirely at fault and intent may be accumulated across the company.[30] Finally, the prosecution of an individual is not a prerequisite for corporate criminal liability.[31]

The only two affirmative defences under the FCPA are that: (1) the payment was lawful under the written laws of the foreign country (the "local law" defence), and (2) the money was spent as part of demonstrating a product or performing a contractual obligation (the "reasonable and *bona fide* business expenditure" defence). Because these are affirmative defences, the defendant bears the burden of proving them.[32]

### 3.2. UK law

Emphasising the separate legal personality doctrine, in a landmark UK corporate law case, *Salomon v A Salomon & Co Ltd*, Lord Macnaghten stated that:

> The company is at law a different person altogether from the subscribers [...] and, though it may be that

[19] See, e.g., *United States v. Dye Constr. Co.*, 510 F.2d 78 (10th Cir. 1975); *Tex.-Okla. Express, Inc. v. United States*, 429 F.2d 100 (10th Cir. 1975); *Riss & Co. v. United States*, 262 F.2d 245 (8th Cir. 1958); *United States v. George F. Fish, Inc.*, 154 F.2d 798 (2nd Cir. 1946).

[20] See, e.g., *United States v. Twentieth Century Fox Film Corp.*, 882 F.2d 656 (2nd Cir. 1989); *United States v. Hilton Hotels Corp.*, 467 F.2d 1000 (9th Cir. 1972), cert. denied 409 U.S. 1125 (1973); *United States v. Ionia Mgmt. S.A.*, 555 F.3d 303 (2nd Cir. 2009).

[21] US Sentencing Commission, Sentencing of Organizations, §8C2.5.

[22] See, e.g., *United States v Bank of New England, N.A.*, 821 F.2d 844 (1st Cir. 1987), at 856.

[23] Yates, *Individual Accountability for Corporate Wrongdoing* (2015).

[24] Mark, *The Yates Memo*, Vol. 51(2018), at 1591.

[25] Gutterman, *Yates Memo Signals Heightened Focus of DOJ on Executives and Other Personnel of Corporate Wrongdoers* (2016).

[26] DOJ, *Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act* (2018), available at: https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0 (last visited on 14 May 2019).

[27] Ibid.

[28] Criminal Division of the US Department of Justice and the Enforcement Division of the US Securities and Exchange Commission, *A Resource Guide to the U.S. Foreign Corrupt Practices Act* (2012), available at: https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf (last visited on 14 May 2019), at 27.

[29] Ibid.

[30] American Criminal Law Review, *Corporate Criminal Liability* (2009), at 369.

[31] Moyer, *Joint DOJ-SEC Guidance on FCPA Clarifies and Confirms Agency Enforcement Attitudes and Policies* (2012).

[32] Ibid., at 23.

> after incorporation the business is precisely the same as it was before and the same persons are managers and the same hands receive the profits, the company is not in law the agent of the subscribers or trustee for them. Nor are the subscribers, as members, liable in any shape or form, except to the extent and in the manner provided by the Act.[33]

More recently, the Legal Guidance on Corporate Prosecutions issued by the UK Crown Prosecution Service (the "CPS Guidance") established the overarching principle pursuant to which, in the absence of legislation which expressly creates criminal liability for companies, corporate liability may be established by either: (1) vicarious liability for the acts of a company's employees/agents, or (2) non-vicarious liability arising from the so-called "directing mind" principle, which determines whether the offender was a directing mind and will of the company.[34]

Vicarious liability will typically arise from offences of strict liability, which do not require intention, recklessness or even negligence as to one or more elements in the *actus reus*. In this case, it is likely that any corporate prosecution will be linked to the prosecution of a controlling officer and/or other employees.[35]

In addition to strict liability offences, companies can also be liable for offences requiring mens rea, whereby "the acts and state of mind" of those who represent the will and directing mind will be imputed to the company.[36] As a starting point, the CPS Guidance instructs prosecutors that, in seeking to identify the "directing mind" of a company, they should consider the constitution of the company in question (by reviewing the company's foundation documents, as well as actions of directors or the company in general meetings) and consider any reference in the company's statutes to offences committed by company's officers.[37]

The "directing mind" test has been criticised as too narrow to deter corporate crime and as encouraging companies to decentralise responsibilities to avoid liability, making it difficult to identify a senior individual who is in charge of a particular operation.[38] For example, in the 2012 LIBOR-fixing scandal, an individual LIBOR-fixer employed by UBS (Hayes) was held liable in a criminal court in England, but UBS itself could not be prosecuted in the UK, because the Serious Fraud Office (SFO) did not have sufficient admissible evidence that a person who was identified as a directing mind was party to Hayes' conduct and therefore could not conclude that there was a realistic prospect of conviction.[39] Moreover, it has been suggested that this test may encourage bad corporate culture and practices, such as manipulation of meeting minutes which fail to record the identity of those present, in order to conceal the presence of board members; and complex organisational structures designed to insulate the board from evidence of wrongdoing.[40]

The one exception to the applicability of the "directing mind" doctrine particularly relevant to MDBs' sanctions regime is Section 7 of the UK Bribery Act 2010, which introduces wider liability in the context of bribery, without requiring the identification of the "directing mind", for failure by a company to prevent bribery by persons associated with it to obtain or retain business or to obtain or retain an advantage in the conduct of business for that commercial organisation, which is very similar to the strict liability under the FCPA. Thus, while a company itself will not be held liable for a bribery offence, it will be guilty of a separate offence of failing to prevent bribery. This is different from the FCPA, where a company can be held vicariously liable for acts of its employees and agents. Further, under the Bribery Act, the company will have a full defence if it can demonstrate that it had adequate procedures in place to prevent persons associated with it from bribing, which is also different from the FCPA approach that does not offer this type of defence and affords only mitigation of sentence for remediation. The question of whether an organisation had adequate procedures in place to prevent bribery in the context of a particular prosecution is a matter that can only be resolved by the courts taking into account particular facts and circumstances of the case. The onus remains on the company to prove that it had adequate procedures in place to prevent bribery.[41]

The government has indicated that the following six core principles demonstrate the existence of adequate procedures: (1) risk assessment, (2) proportionality of risk-based prevention procedures, (3) top level commitment, (4) due diligence in respect of persons who perform services for or on behalf of the organisation, (5) communication throughout the organisation (including training) and (6) monitoring and review.[42]

The principle of holding a company liable for its employees' offences was illustrated in the first conviction of a company under the Bribery Act, which occurred in February 2016, when a construction and professional services company, Sweett Group PLC pled guilty to a charge of failing to prevent bribery by its subsidiary's employees in the Middle East. In sentencing, the judge described the offence as a system failure patently committed over a period of time.[43] Interestingly, some have criticised the fact that no individuals have been charged in relation to corporate wrongdoings in the *Sweett* and other similar

[33] *Salomon v A Salomon & Co Ltd* [1896] UKHL 1.

[34] Corporate Prosecutions: Legal Guidance: The Crown Prosecution Service, available at: http://www.cps.gov.uk/legal/a_to_c/corporate_prosecutions/ (last visited on 14 May 2019), ¶10.

[35] Ibid., ¶16.

[36] Ibid., ¶17

[37] Ibid., ¶20.

[38] Ministry of Justice, Corporate Liability for Economic Crime, Call for evidence (2017), at 13.

[39] Ibid., at 14.

[40] Ibid.

[41] UK Ministry of Justice Guidance on the UK Bribery Act 2010, available at: https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf (last visited on 14 May 2019), at 6.

[42] Ibid., at 21-31.

[43] SFO, *Sweett Group PLC sentenced and ordered to pay £2.25 million after Bribery Act conviction* (2016).

cases.[44] As described in Section 3.1 above, it was exactly this type of criticism for leaving senior executives untouched that led to the increased emphasis on individual accountability by the DOJ.

More recently, the Criminal Finances Act 2017 came into force and, similar to the Bribery Act, introduced an offence of the failure to prevent facilitation of tax evasion. If a person "associated with" the relevant company commits the offence, the company will be vicariously liable.[45] Just like the Bribery Act, the Criminal Finances Act provides for a defence where, at the time of the offence, the company had in force "reasonable prevention procedures".[46] Thus, it would appear that the government is moving away from the "directing mind" doctrine and imposing strict liability on companies accused of facilitating tax evasion, unless they can demonstrate that they had adequate prevention procedures in place.

### 3.3. Application of the foregoing principles to MDBs' sanctions procedures

While the Principles' general stance towards the sanctioning of companies that employ sanctioned respondents is in line with the ethos of the FCPA and the UK Bribery Act, MDBs' sanctions regimes would benefit from greater clarity in this area. In particular, without further clarification, the "failure to supervise" could incentivise companies to argue that they had properly supervised their employees, but that the employees acted "rogue" in committing a sanctionable practice.[47]

To that end, two distinct bases of liability emerge as an option for MDBs' sanctions regimes: (i) the vicarious liability under the FCPA and (ii) the strict liability under the UK Bribery Act for failure to prevent a sanctionable practice. As is generally the case with all options, each of the two has its advantages and disadvantages. Specifically, under the vicarious liability doctrine, a company would be liable for a sanctionable practice of its culpable employee if (s)he acted within the scope of his/her employment and with the intent to benefit the company.

One of the main problems with vicarious liability is that an individual who commits wrongful acts could simultaneously be held individually responsible for them. Arguably, this can give the appearance of scapegoating, particularly if it is the company's culture (which is set by the management) that condones or even encourages corrupt practices.[48] On the other hand, the risk of relying solely on impersonal corporate liability is that corporate sanctions are ineffective in eliciting a sufficient corporate response to non-compliance by simply replacing management without addressing the underlying problem. Therefore, in addition to imposing a sanction on a company for a sanctionable practice committed by its employees, a vicarious liability regime should also emphasise the strong behavioural influence of corporate management and adequate procedures to prevent misconduct.[49]

By contrast, the regime that holds companies strictly liable for sanctionable practices committed by employees undermines the companies' ability to deter corporate misconduct, because it would hold companies liable for sanctionable practices committed by their employees within the scope of employment, regardless of the efforts and resources mobilised by the company.[50] For example, a company that has detected misconduct could report it and cooperate with the authorities; however, by doing so, the company should expect to be convicted for its employees' wrongdoing.[51]

In order to avoid companies being caught on the horns of such dilemma, the UK Bribery Act gives companies a full defence if they can demonstrate that they had adequate procedures in place to prevent their employees' misconduct, thus practically turning the strict liability standard into a negligence standard. This approach, however, is also problematic because what constitutes "adequate procedures" will depend on the unique risks and challenges of each organisation and, despite the UK government's broad-brush guidelines on the indicia of adequate procedures, law enforcement authorities, let alone MDBs, are not necessarily best placed to determine whether a company's procedures adequately address the risks presented. In addition, the company is best placed to argue why its systems work despite the violation that occurred, while in fact, the occurrence of a violation should serve as an indicator that the company's procedures could be improved. Moreover, offering companies complete exoneration from liability if they have put "adequate procedures" in place may also incentivise companies to focus on adopting measures that are easily demonstrable to the authorities, such as elaborate policies and formal trainings, rather than focusing on adopting the most effective measures, such as the creation of the culture of integrity from the top.

Additionally, it has been suggested that compliance programmes are not sufficient in and of themselves and that companies need to do such additional measures as: (i) reforming compensation/promotion/retention policies to ensure that they encourage productivity without also encouraging misconduct, (ii) self-reporting all detected misconduct and (iii) fully cooperating by investigating the wrongdoing and turning over all materials to the enforcement authorities. Otherwise, arguably, regimes that exonerate companies from liability if they have an effective compliance programme do not provide companies with

[44] OECD, *Public Consultation on Liability of Legal Persons: Submission by Corruption Watch*, United Kingdom (2016), at 40.

[45] Criminal Finances Act 2017, §§44-46.

[46] Ibid., §§45 and 46.

[47] See, e.g., OECD, *Public Consultation on Liability of Legal Persons: Submission by Chiawen Kiew and Melissa Khemani* (2016), at 76.

[48] See, e.g., OECD, *Public Consultation on Liability of Legal Persons: Submission by U4 Anti-Corruption Resource Centre* (2016), at 11.

[49] Ibid.

[50] OECD: *Public Consultation on Liability of Legal Persons: Submission by Jennifer Arlen* (2016), at 7.

[51] Ibid.

needed incentives to self-report, fully cooperate or take other actions to deter crime (such as compensation and promotion policy reform).[52]

In light of the above, it might be better for the existence of effective procedures to be considered as a mitigating factor in assessing the appropriate sanction that should be imposed, rather than a full defence, as under the UK Bribery Act. Thus, a desirable MDBs' system for holding companies liable for sanctionable practices committed by their employees should deter companies from engaging in sanctionable practices while motivating them to effectively exercise control over their employees. This could be achieved by a hybrid system that would start off with strict liability (i.e., holding companies strictly liable for sanctionable practices committed by their employees in the scope of employment, even if the company did all it reasonably could to prevent the wrongdoing), while rewarding companies–through the use of mitigating factors–for measurable actions to prevent the occurrence of sanctionble practices, as well as for voluntarily self-reporting and cooperating with the investigation. Only where a company could show that there was no failure to supervise and that appropriate measures were taken as soon as the wrongdoing was discovered, could this lead to further mitigating factors and possibly even provide grounds for exculpation. Such measures would also need to be accompanied by self-reporting and cooperation with the investigation; otherwise, if companies were protected from liability on the grounds of having an effective compliance programme, this would not create incentives for companies to self-report and fully cooperate.

MDBs could also provide some guidance on how to determine whether a company's compliance system was adequately designed and implemented. A good example is the FCPA Resource Guide by the DOJ and the Securities Exchange Commission (SEC), which describes the ten "hallmarks of effective compliance program", which include: (i) commitment from senior management and a clearly articulated policy against corruption; (ii) clear, concise and accessible code of conduct and compliance policies and procedures; (iii) proper authority, autonomy from management and adequate resources by the responsible manager; (iv) risk-based approach, with greater focus on high-risk areas than on low-risk markets; (v) local language training, with web-based or in-person delivery, tailored to particular jobs and situations with relevant hypotheticals; (vi) incentives and disciplinary measures, where staff are rewarded for ethics and compliance leadership and disciplinary measures for misconduct; (vii) due diligence of agents, consultants and distributors, which entails: (a) understanding the parties' qualifications and associations, (b) understanding the business rationale for including them in the transaction and (c) undertaking ongoing monitoring; (viii) reporting mechanism that allow for confidentiality and protect against retaliation; (ix) regular review and improvements of the compliance programme; and (x) in the context of mergers and acquisitions, a robust FCPA due diligence of the target company and prompt integration of the acquired company into the acquiring company's internal controls, including its compliance programme.[53]

## 4. Liability of a parent for its subsidiaries' wrongdoings

The typical corporate group includes one or more parent companies that hold a majority or controlling equity interest in one or more subsidiaries, which together function as a single economic enterprise, often with a common public identity.[54] Regardless of how the boundaries of the corporate group are defined, each subsidiary within the corporate group enjoys separate legal personality from its shareholder parent. More often than not, however, the decision to form a subsidiary, as opposed to an internal division within a company, is driven by tax, regulatory or managerial factors.[55] A corporate group's organisational structure is therefore not an accurate indicator of the group's economic organisation or actual decision-making authority within the group. In an equity-based corporate group, one or more parent entities generally exercise control of subsidiaries through voting control, which often, but not always, corresponds to the parent entity's financial stake.[56] The parent(s) also exercise(s) direct or indirect control of subsidiary management through operational integration, overlapping directors and officers, or contractual means.[57] A significant equity stake in a higher-tier subsidiary may be enough to convey effective control over lower-tier subsidiaries, which may be wholly owned or partially owned by the parent.[58]

The following Sections analyse the liability of a parent company for its subsidiaries' wrongdoing under the US and UK law, and make suggestions for enhancements of the Principles.

### 4.1. US law

#### 4.1.1. General Approach

With respect to piercing the corporate veil from subsidiary to parent, it has been suggested that the "traditional 'piercing' jurisprudence rests on a demonstration of three fundamental elements: (1) the subsidiary's lack of independent existence; (2) the fraudulent, inequitable, or wrongful use of the

[52] Ibid., at 9.

[53] Criminal Division of the US Department of Justice and the Enforcement Division of the US Securities and Exchange Commission, supra note 28, at 57-68.

[54] Blumberg, *The Transformation of Modern Corporation Law: The Law of Corporate Groups* (2005), at 606.

[55] Harper Ho, *Of Enterprise Principles and Corporate Groups: Does Corporate Law Reach Human Rights?* (2013-2014), at 133.

[56] Ibid., at 134.

[57] Ibid.

[58] Ibid.

corporate form; and (3) a causal relationship to the claimant's loss. Unless each of these three elements has been shown, courts have traditionally held "piercing" unavailable." [59]

The first element contemplates a lack of real-world existence of the subsidiary resulting from an exercise by the parent of such a high degree of control over the affairs of the subsidiary that it is reduced to a "mere agency" of the parent, comparable to a division.[60] The second element is a use by the parent of the subsidiary for an improper purpose that amounts to an abuse of the privilege of carrying on business as a corporation.[61] The final factor requires a claimant to show a causal connection between the defendant's wrongful act and the injury sustained by the claimant.

Unfortunately, it does not seem that the tests used by courts to determine the existence of these elements are entirely clear. Namely, the application of these tests often consists largely of lists that courts recite, which has resulted in a number of overlapping lists of factors that are passed off as tests.[62] For example, in *Victoria Elevator C. v Meridian Grain Co*, the court listed the following factors: (1) insufficient capitalisation for purposes of corporate undertaking, (2) failure to observe corporate formalities, (3) non-payment of dividends, (4) insolvency of debtor corporation at time of transaction in question, (5) siphoning of funds by dominant shareholder, (6) non-functioning of other officers and directors, (7) absence of corporate records and (8) existence of corporation as merely a façade for individual dealings.[63]

Scholars have suggested that "[t]his is one of the most unsatisfactory areas of the law. With hundreds of irreconcilable decisions and shifting rationales, it functions in an almost inscrutable manner behind conclusory metaphors such as 'mere instrumentality', 'sham', 'adjunct', 'agent', 'alter ego', 'puppet' or dozens of similarly murky terms."[64] Specifically, courts have held a parent company liable for the actions of a subsidiary pursuant to the regulatory policies of the Federal Water Pollution Prevention and Control Act,[65] the Robinson-Patman Act (the anti-price discrimination law),[66] the Federal Trade Commission Act,[67] and the Commodity Exchange Act,[68] among others. However, they have not used a single test; rather, federal regulatory policies have resulted in a broad range of tests used, with courts often citing public interest concerns as key in their determination of whether a parent company should be found liable for the acts of its subsidiaries. Thus, for example, in *P.F. Collier & Son Corp. v F.T.C.*, which concerned the Federal Trade Commission Act, the court held:

Manifestly, where the public interest is involved, as it is in the enforcement of Section 5 of the Federal Trade Commission Act, a strict adherence to common law principles is not required in the determination of whether a parent should be held for the acts of its subsidiary, where strict adherence would enable the corporate device to be used to circumvent the policy of the statute.[69]

The court found the following factors relevant in finding the parent's liability: the parent not only wholly-owned the relevant subsidiaries, but also (i) interchanged personnel with its subsidiaries and maintained common or overlapping officers and directors; (ii) operated through its subsidiaries, which were often created and dissolved for purposes unrelated to the business carried on by the corporate complex; and (iii) approved the use by its subsidiaries of the parent's name and goodwill in order to develop favourable public associations between the parent and its subsidiaries.

#### 4.1.2. Criminal liability, including FCPA

The problem with establishing the criminal liability of a parent company for criminal acts of its subsidiary is that many economic crimes require a mental element (such as an intention to commit an offence or *mens rea*). Nonetheless, federal law permits prosecution of the parent if it exercises sufficient control over the subsidiary under the same *respondeat superior* doctrine described in Section 3.1 above. Thus, just as a corporation may be responsible for the criminal acts of its employees when they act for the corporation, so is subsidiary sometimes treated as the legal agent of the parent.[70]

Specifically, under the **agency theory of liability**, a parent may be liable for the acts of its subsidiary because the subsidiary's employees are considered either agents or sub-agents of the parent.[71] A subsidiary's employee may become the parent's agent if the parent has taken some demonstrable step that effectively authorises that employee to act as the parent's agent for the type of activity in which the illegal conduct occurred. Alternatively, under the vicarious liability doctrine, a subsidiary could be viewed as the parent's agent when the illegal conduct occurred.[72]

---

[59] Matheson, *The Modern Law of Corporate Groups: An Empirical Study of Piercing the Corporate Veil in the Parent-Subsidiary*, Vol. 8, (2009), at 1099, citing Blumberg, *The Law of Corporate Groups: Procedural Problems in the Law of Parent and Subsidiary Corporations* (1983), at 612.

[60] Blumberg et al., *Blumberg on Corporate Groups* (2013-2012), § 10.03[B], at 8.

[61] See *Oddenino & Gaule v. United Fin. Group*, 1999 U.S. App. LEXIS 29506, Ninth Cir. (November 1999), at 3.

[62] Ibid.

[63] *Victoria Elevator Co. v Meridian Grain Co.*, 283 N.W.2d 509 (1979).

[64] Blumberg, *Accountability of Multinational Corporations: The Barriers Presented by Concepts of the Corporate Juridical Entity* (2001), at 307.

[65] See, e.g., *United States v Ira S. Bushey & Sons, Inc.*, 363 F. Supp. 110 (D. Vt. 1973).

[66] See, e.g., *Reines Distribs., Inc. v. Admiral Corp.*, 256 F. Supp. 581 (S.D.N.Y. 1966).

[67] See, e.g., *P.F. Collier & Son Corp. v F.T.C.*, 427 F.2d 261 (6th Cir. 1970).

[68] See, e.g., *Corn Prods Refining Co. v Benson*, 232 F.2d 554 (2nd Cir. 1956).

[69] *P.F. Collier & Son Corp. v F.T.C.*, supra note 67, at 267.

[70] See, e.g., *United States v Bestfoods*, 524 U.S. 51, 62-65 (1998) (federal).

[71] See Conspiracy to commit offense or to defraud United States, 18 U.S. Code § 371.

[72] Poindexter, *Criminal and Civil Liability for Corporations, Officers and Directors* (2016).

Under the **mere instrumentality or unity of business theory of liability**, a parent may be held liable for its subsidiary's misconduct when the parent uses the subsidiary to violate the law and does not treat the subsidiary as a separate entity.[73] Courts consider several factors in determining whether to impute the actions of a subsidiary to its parent, including whether: the parent and subsidiary have common officers and directors; the parent and subsidiary have consolidated financial statements; the subsidiary is grossly undercapitalised; the parent finances the subsidiary; the subsidiary receives only the parent's business; the parent uses the subsidiary's property as its own; the daily operations of the parent and subsidiary are not separate (for example, both companies are located in the same building and use the same equipment); and the parent and subsidiary fail to observe corporate formalities, such as required shareholder meetings.[74]

However–and this is particularly relevant in the context of MDBs' sanctions regimes–authorities have been quick to hold parent companies liable for their subsidiaries' violations of the FCPA. In that context, in the FCPA Resource Guide, the DOJ and the Securities and Exchange Commission (SEC) have provided the following guidance:

> There are two ways in which a parent company may be liable for bribes paid by its subsidiary. First, a parent may have participated sufficiently in the activity to be directly liable for the conduct—as, for example, when it directed its subsidiary's misconduct or otherwise directly participated in the bribe scheme.
>
> Second, a parent may be liable for its subsidiary's conduct under traditional agency principles. The fundamental characteristic of agency is control. Accordingly, DOJ and SEC evaluate the **parent's control** [emphasis added]—including the parent's **knowledge and direction** [emphasis added] of the subsidiary's actions, both generally and in the context of the specific transaction— when evaluating whether a subsidiary is an agent of the parent.
>
> Although the formal relationship between the parent and subsidiary is important in this analysis, so are the practical realities of how the parent and subsidiary actually interact. If an agency relationship exists, a subsidiary's actions and knowledge are imputed to its parent. Moreover, under traditional principles of respondeat superior, a company is liable for the acts of its agents, including its employees undertaken within the scope of their employment and intended, at least in part, to benefit the company. Thus, if an agency relationship [emphasis added] exists between a parent and a subsidiary, the parent is liable for bribery committed by the subsidiary's employees.[75]

Case law suggests that the standard is rather low for the SEC to determine that a parent company controlled a subsidiary for purposes of finding that the parent company should be liable for its subsidiary's FCPA violation. For example, in 2014, the SEC found Alcoa Inc. liable for corrupt practices of its subsidiaries under agency principles. In determining that Alcoa's subsidiaries were agents of the parent company, the SEC considered the following factors: First, Alcoa appointed the majority of seats on a Strategic Council that provided "direction and counsel" to the subsidiaries. Second, Alcoa and a subsidiary transferred personnel between them. Third, Alcoa set the business and financial goals for the subsidiaries and coordinated their legal, audit and compliance functions. Fourth, the subsidiaries' employees managing the business with the company involved in the corrupt scheme (Alba) reported functionally to Alcoa officials. Fifth, Alba was a significant Alcoa customer. Sixth, members of Alcoa senior management met with Alba officials and a consultant involved in the scheme to discuss matters related to the Alba relationship. Seventh, Alcoa officials were aware that the consultant was the subsidiaries' agent and that the terms of related contracts were reviewed and approved by senior Alcoa managers.[76]

The first five factors relate to the parent company's influence over the subsidiaries generally and not in connection with the alleged wrongdoing. The sixth and seventh factors are described quite neutrally and there does not seem to be any indicia of Alcoa's management taking inappropriate actions with respect to the consultant in question. If these factors suffice to establish parent liability under the FCPA, many subsidiaries are likely to be considered parent company's "agents".

Similarly, in 2016, the SEC found SciClone Pharmaceuticals, Inc., a California-based company, liable for its Chinese subsidiary's FCPA violation. In finding that SciClone controlled its subsidiary, the SEC noted that:

> SciClone directs the relevant operations of SPIL [the subsidiary] and its subsidiaries and oversees SPIL's operations through various means including through the appointment of directors and officers of SPIL, review and approval of its annual budget, business and financial goals and oversight of its legal, audit and compliance functions. SciClone also reviews and approves annual marketing and promotion budgets of SPIL and its subsidiaries. During relevant periods, some SciClone officers also served as officers and/or directors of SPIL, travelled frequently to China to participate in the management of SPIL.[77]

These factors also appear quite neutral and do not entail any pleading by the parent company in the subsidiaries' FCPA violations. Finally, in November 2016, the SEC found JPMorgan liable for the FCPA violation of its Chinse subsidiary JPMorgan APAC, which was found to have won business from clients and corruptly influenced government officials in the Asia-Pacific region by giving jobs and

[73] See *NLBR v Deena Artware, Inc.*, 361 U.S. 398 (1960), at 402-403 and *United States v Jon-T Chems, Inc.*, 768 F.2d 686 (5th Cir. 1985), cited in Poindexter.

[74] Poindexter, supra note 72.

[75] Criminal Division of the US Department of Justice and the Enforcement Division of the US Securities and Exchange Commission, supra note 28, at 27-28.

[76] SEC Cease-and-Desist Order in the matter of Alcoa Inc. (9 January 2014), available at: https://www.sec.gov/litigation/admin/2014/34-71261.pdf (last visited on 14 May 2019), at 10.

[77] SEC Administrative Proceeding File No. 3-17101, *In the Matter of SciClone Pharmaceuticals, Inc.* (4 February 2016).

internships to their relatives and friends.[78] Even though the SEC recognised that "JPMorgan APAC employees failed to follow the firm's internal accounting controls [...] and took steps to hide the magnitude and purpose of the Client Referral Program from others within the firm and devised a way to avoid having certain Referral Hires in APAC counted within JPMorgan APAC's internal year-end headcount calculations", it still found JPMorgan liable because it "failed to devise and maintain a system of internal accounting controls around its hiring practices sufficient to provide reasonable assurances that its employees were not bribing foreign officials in contravention of company policy".[79] Thus, it would appear that inadequate proceedings for the prevention of the FCPA activities will result in the parent company's liability, without the SEC necessarily finding the parent company's knowledge about the subsidiary's actions.

#### 4.1.3. Proposals for reforms of the US system

It has been suggested that the test for finding the existence of an enterprise should have at its basis an enquiry of economic control, focusing on the integration of parent and subsidiary companies to pursue one economic purpose.[80] In that context, the relevant enquiries might include whether: (1) the subsidiary exists in order to further the economic goals of the parent, (2) the corporate group presents itself to the public as a unified enterprise through, for example, common logos, policies and guiding principles, (3) the two companies are functionally part of the same business and, most importantly, (4) the subsidiary was created or is utilised to advance business goals of the parent company, in order to essentially externalise the parent company's risk.[81] Each of these questions is aimed at determining the functional economic integration of the two companies.

Still, the problem with trying to determine the functional economic integration of the two companies and elements of the parent company's control over a subsidiary is that, the further down the chain we are, the more difficult it becomes to establish the elements of control, which points to the deficiencies of the control/agency theory.

Basing her findings on several international corporate liability regimes, Dearborn thus advocates that the company should bear the burden in disproving the existence of an enterprise, without the claimant having to prove the economic structure of the corporate group.[82] Therefore, once the claimant demonstrates to the court that it was harmed by an activity of the corporate group and that the parent and subsidiary were both members of that group, the company should have to prove that it is not part of an economic enterprise. The main reason for this shifting of the burden of proof is that the parent company has better access to information about the internal structure of the group than the claimant.[83] While this seems logical, merely looking at the corporate structure without considering other factors, such as, for example, control and operational arrangements, is quite a simplistic approach, which has been criticised by the UK courts, as described in continuation.

### 4.2. UK law

#### 4.2.1. General approach

The fundamental principle in the UK is that "each company in a group of companies is a separate legal entity possessed of separate legal rights and liabilities".[84] However, courts have developed certain exceptions for finding a parent company liable for its subsidiaries' actions. Thus, in a landmark corporate law case, *Adams v Cape Industries plc*, in which an English company was sued for the actions of one of its subsidiaries in South Africa, the court set forth three main grounds for veil piercing: (1) a single economic unit, when a group of companies should be treated as a single economic entity; (2) special circumstances that point to subsidiaries being a mere façade to the true group dynamics; and (3) agency.[85]

In this particular case, the court rejected all three grounds. More specifically, with respect to a single economic entity, the court established that corporate veil should not be pierced just because a group of companies operated as a single economic unit. The court pointed out that:

> [T]he court is [not] entitled to lift the corporate veil as against a defendant company which is the member of a corporate group merely because the corporate structure has been used so as to ensure that the legal liability (if any) in respect of particular future activities of the group (and correspondingly the risk of enforcement of that liability) will fall on another member of the group rather than the defendant company. Whether or not this is desirable, the right to use a corporate structure in this manner is inherent in our corporate law.[86]

Further, the court accepted that the veil could be lifted if the subsidiary was a mere façade concealing the true facts, but did not find that this applied to the company at hand. Similarly, the court did not find any evidence of the agency relationship, given that the subsidiaries were independent and with no general power to bind the parent and held that such an agency relationship can be established only where there was an express agency agreement between the companies.[87]

---

[78] SEC Press Release, *JPMorgan Chase Paying $264 Million to Settle FCPA Charges* (17 November 2016).

[79] SEC Administrative Proceeding File No. No. 3-17684, *In the Matter of JPMorgan Chase & Co.* (17 November 2016).

[80] Dearborn, *Enterprise Liability: Reviewing and Revitalizing Liability for Corporate Groups*, Vol. 97 (February 2009), at 252.

[81] Ibid., at 252-253.

[82] Ibid., at 253.

[83] Ibid

[84] Sealy, *Cases and Material in Company Law* (2001), at 71.

[85] *Adams v Cape Industries plc* [1990] Ch 433.

[86] Ibid.

[87] No.5 Barristers Chambers, Piercing the Corporate Veil 2010 (January 2011).

Despite this apparent tendency of UK courts to strictly follow the separate legal personality and limited liability doctrine laid down in *Salomon*, the more recent cases, particularly in connection with criminal liability and the UK Bribery Act violations, suggest a greater tendency to hold parent companies liable for their subsidiaries' illegal actions.

#### 4.2.2. Criminal liability, including UK Bribery Act

As in the US, the problem with establishing the criminal liability of a parent company for criminal acts of its subsidiary is that many economic crimes require a mental element (such as an intention to commit an offence or *mens rea*) and there is an inherent difficulty in establishing corporate criminal liability for such offences and attributing a human state of mind, such as intention, to a company."[88]

In recent years, two important pieces of legislation have sought to overcome the historical difficulty of establishing corporate criminal liability by creating specific corporate offences: (1) corporate manslaughter (Corporate Manslaughter and Corporate Homicide Act 2007 (CMCHA)) and (2) failure to prevent bribery (Bribery Act 2010), the latter being particularly relevant for MDBs' sanctions regimes.[89]

Under the CMCHA, an organisation is guilty of an offence if the way in which its activities are managed or organised (i) causes a person's death and (ii) amounts to a gross breach of a relevant duty of care owed by the organisation to the deceased.[90] Section 8 of the CMCHA allows the jury to consider the attitudes, policies, systems or accepted practices that were likely to have encouraged the breach or produced a tolerance of it.

As described in Section 3.2 above, under Section 7 of the UK Bribery Act, a company is liable for the offence of failing to prevent bribery. Similar to the FCPA, Section 7 of the Bribery Act says that a company is guilty of an offence if a *person associated with it* bribes another person intending to obtain or retain business for the organisation. The Ministry of Justice's Guidance on the Bribery Act clarifies the scope of parent company's liability for its subsidiaries' violations as follows:

> [A] bribe on behalf of a subsidiary by one of its employees or agents will not automatically involve liability on the part of its parent company, or any other subsidiaries of the parent company, if it cannot be shown the employee or agent intended to obtain or retain business or a business advantage for the parent company or other subsidiaries. This is so even though the parent company or subsidiaries may benefit indirectly from the bribe. By the same token, liability for a parent company could arise where a subsidiary is the 'person' which pays a bribe which it intends will result in the parent company obtaining or retaining business or vice versa.[91]

Clearly, the mere fact of a parent and subsidiary relationship will not automatically result in the finding that the subsidiary is performing services for and on behalf of the parent. Rather, it will be necessary to demonstrate that the subsidiary acted with the intention of obtaining an advantage for the parent. This is a higher standard than that applied by the SEC, as described above. The SFO managed to demonstrate this in its first conviction under Section 7, when in 2016 it convicted Sweett Group PLC (a UK-based company) for the offence of failing to prevent its subsidiary from paying bribes on its behalf in the Middle East. Sweett was unable to rely on the defence of having adequate procedures in place to prevent bribery.[92]

Section 7 liability is not limited to a parent company. As illustrated by the SFO first deferred prosecution agreement with Standard Bank PLC, it can also extend to other companies within the corporate group. In that case, Standard Bank's Tanzanian sister company, Stanbic Bank Tanzania was charged with bribing a local partner in Tanzania to induce members of the government to favour Stanbic's private placement proposal. However, given that both sister companies stood to benefit from the transaction (with the fee split 50/50) and were acting jointly (with different but complementary roles), the employees and the Tanzanian company were regarded as associated persons of the UK company and their bribery act regarded as benefitting both companies.[93]

In conclusion, where corporate groups are involved, *Salomon* remains the starting point in UK courts. However, courts have been more willing to lift the veil recently, especially where personal injury or criminal liability is involved. This seems fair, as otherwise shareholders would enjoy double protection.

### 4.3. Application of the foregoing principles to MDBs' sanctions procedures

As described in Section 2 above, the Principles recommend that sanctions be applied to a respondent's parent company if the parent company was involved in the sanctioned misconduct, including as a result of wilful blindness and failure to supervise. Both concepts are problematic and require further guidance: Wilful blindness itself is quite a fluid concept and, as described above, jurisdictions vary in the information that may be considered to infer the parent's guilt.[94] As with the "failure to supervise" employees, described in Section 3 above, the "failure to supervise" a subsidiary could easily incentivise companies to argue that they had properly

[88] Grimes, Niblock and Madden, *Corporate criminal liability in the UK: the introduction of deferred prosecution agreements, proposals for further change, and the consequences for officers and senior managers* (2013/14).

[89] Ibid.

[90] CMCHA § 1(1).

[91] Ministry of Justice, *UK Bribery Act Guidance*, supra nota 41, at 45.

[92] SFO, supra note 43.

[93] *SFO v Standard Bank,* Royal Courts of Justice, PLC Case No: U20150854 (30 November 2015).

[94] Baldwin Jr. and Koslosky, *Mission Creep in National Security Law* (2012), at 689.

supervised their subsidiaries, but that the employees of the relevant subsidiary acted "rogue" in committing a sanctionable practice.[95] Thus, it would be important to distinguish between the parent's culpability based on the **actual knowledge and deliberate participation** in the wrongdoing, on the one hand and organisational responsibility, on the other hand, which may arise from a failure to supervise or to maintain adequate controls or ethical culture within the corporate group, such that the wrongdoing is made possible. The former should result in a sanction, although knowledge will obviously thin out the longer the chain of entities between the parent company and the ultimate subsidiary becomes. Each analysis of the relationship between the parent and the subsidiary will be fact-specific and MDBs could take guidance from the FCPA Resource Guide and the US case law regarding the factors considered in determining the level of the parent's control. The greater such control, the easier it will be to establish that a subsidiary's misconduct was intended to benefit the parent company, if one is also to apply the above-described UK Ministry of Justice's Guidance.

On the other hand, mere responsibility should not normally lead to debarment, but instead to conditional non-debarment. Under this sanction, the parent company would not be debarred, but would have to comply with certain conditions and report on its compliance to the MDB for a period of time. This way, an MDB could require that companies develop and implement effective anti-corruption compliance systems as a condition of non-debarment, which would allow the MDB to help a company reform its controls and at the same time avoid imposing a sanction that may have draconian consequences for the company, the market, the project and the community at large. As described in Section 3.3 above, the FCPA Resource Guide lists some useful factors to determine the adequacy of a company's compliance programme.

## 5. Liability of a subsidiary for its parent's wrongdoings

### 5.1. US and EU sanctions regimes

As noted above, the Principles state a rebuttable presumption that sanctions should be applied to all entities controlled by the respondent, unless the respondent demonstrates that the entities are free of responsibility for the misconduct, application to the entities would be disproportional and is not reasonably necessary to prevent evasion. Interestingly, MDBs seem to follow slightly different guidelines on what constitutes "control". For example, ADB's Integrity Principles and Guidelines say that, in determining interest or control, the investigators will consider, among other things, "the degree of association, proximity of the sanctioned party and the similarity of business activities or operations with the sanctioned party".[96] EBRD's Enforcement Policy and Procedures say that "the indicia of "control" include, but are not limited to, the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of another entity, whether through the ownership of voting shares, by contract or otherwise".[97] Finally, the WB's Information Note says that the indicia of "control" include, but are not limited to, interlocking management or ownership, identity of interests among family members, shared facilities and equipment, common use of employees, or a business entity organised following the imposition of a sanction that has the same or similar management, ownership, or principal employees as the person that was suspended or debarred.[98]

When considering further guidance on imposing a sanction on the respondent's subsidiaries, it is worth analysing the US and the UK economic sanctions. In that context, the US Treasury Department's Office of Foreign Assets Control (OFAC) applies the "50% rule", pursuant to which any company that is owned 50% or more by a blocked person or entity, is blocked even if the company itself is not on the OFAC list of sanctioned parties.[99]

Further, OFAC aggregates the ownership interests of sanctioned parties when determining whether the 50% rule applies. For example, if a Blocked Person X owns 25% of Entity A and a Blocked Person Y also owns 25% of Entity A, then Entity A is blocked, because it is owned 50% or more in the aggregate by blocked persons. Aggregation applies even if Person X and Person Y are blocked under different sanctions programmes.[100] In addition, the application of the 50% rule to indirect ownership interests will result in a cascade-down effect. For example, if Blocked Person X owns 50% of Entity A and Entity A owns 50% of Entity B, both Entity A and Entity B are automatically blocked.[101]

Notably, however, the US sanctions apply only through ownership and not through control, of entities, as is the case with the EU sanctions and MDBs' sanctions.[102] Similarly, the US Bank Holding Company Act provides for a rebuttable presumption of control if a parent or holding company holds 25% of the voting shares of another company, controls the election of the company's directors, or retains the ability to control the management or policies of the company.[103] Likewise, the Savings and Loan Holding Company Amendments Act provides for a rebuttable presumption of control if the parent or controlling company holds 25% of the

[95] See, e.g., OECD, *Public Consultation on Liability of Legal Persons: Submission by Chiawen Kiew and Melissa Khemani* (November 2016), at 76.

[96] ADB, *Integrity Principles and Guidelines* (2015), footnote 26.

[97] EBRD's Enforcement Policy and Procedures, § II(2).

[98] The World Bank Group's Sanctions Regime, Information Note, available at: https://www.worldbank.org/en/about/unit/sanctions-system (last visited on 14 May 2019), at 21.

[99] US Department of the Treasury, *Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property are Blocked* (2014).

[100] See US Department of the Treasury: *OFAC FAQs: General Questions*; see also Willkie, Farr & Gallagher LP: *New OFAC Guidance on 50% Rule Expands U.S. Sanctions Against Russia* (2014).

[101] Ibid.

[102] US Department of the Treasury, supra note 100, Question 398.

[103] 12 U.S.C. § 1841(a)(2).

subsidiary's voting shares.[104] This approach is curious, given that the FAR, on the other hand, applies to "affiliates", which are determined through control and control is a question of fact. The FAR says that the indicia of "control" include, but are not limited to, interlocking management or ownership, identity of interests among family members, shared facilities and equipment, common use of employees, or a business entity organised following the debarment, suspension, or proposed debarment of a contractor which has the same or similar management, ownership, or principal employees as the contract or that was debarred, suspended, or proposed for debarment.[105]

By contrast, the EU Regulation 833/2014, as amended by Regulation 960/2014 ("Regulation 960") mandates that EU persons are prohibited from transacting with an entity that is 50% or more owned by a sanctioned party (which is the same as the OFAC rule), or "controlled" by such party (which is in addition to the OFAC rule). The indicia of control are:

(i) having the right or exercising the power to appoint or remove a majority of the members of the administrative, management or supervisory body of a company;

(ii) having appointed solely as a result of the exercise of one's voting rights a majority of the members of the administrative, management or supervisory bodies of a company who have held office during the present and previous financial year;

(iii) controlling alone, pursuant to an agreement with other shareholders in or members of a legal person or entity, a majority of shareholders' or members' voting rights in that legal person or entity;

(iv) having the right to exercise a dominant influence over a legal person or entity, pursuant to an agreement entered into with that legal person or entity, or to a provision in its memorandum or articles of association, where the law governing that legal person or entity permits its being subject to such agreement or provision;

(v) having the power to exercise the right to exercise a dominant influence referred to in point (iv), without being the holder of that right;

(vi) having the right to use all or part of the assets of a legal person or entity;

(vii) managing the business of a legal person or entity on a unified basis, while publishing consolidated accounts; and

(viii) sharing jointly and severally the financial liabilities of a legal person or entity, or guaranteeing them.

If any of these criteria are satisfied, it is considered that the legal person or entity is controlled by another person or entity, unless the contrary can be established on a case-by-case basis.[106]

### 5.2. Application of the foregoing principles to MDBs' sanctions procedures

Despite the OFAC approach, there are numerous benefits to having "control" defined by actual control and not only a threshold share ownership. Namely, a small, organised group of shareholders, whose combined ownership of shares exceeds 50% of the total number of shares is able to control a company by acting in concert. Also, when share ownership is widely diffused among a large number of shareholders, control may be secured by owning 20% or less of the total shares. Consequently, Regulation 960, together with its indicia of control seems to offer a more nuanced approach to determining true control of a subsidiary.

Finally, with respect to the practical difficulties around the identification of subsidiaries covered by a sanction imposed on a respondent "and all of the entities controlled by it", there are two possible solutions:

(i) First, the creation of a comprehensive database of each of the entities that is sanctioned together with the exact names of all entities controlled by it, similar to the databases maintained by the OFAC and the European Commission. In order to be meaningful, such database would have to be updated regularly in order to capture newly created subsidiaries, which would of course require additional resources.

(ii) Second, whenever a company applies for a project financed by the relevant MDB (be it as a borrower, a contractor, sub-contractor, or in any other capacity in which it stands to benefit from such project), it should be asked to represent in the financing agreements that it is not a subsidiary of any of the entities sanctioned by that MDB. Obviously, this type of self-certification is not as robust as the actual checking of the database, but is less costly and provides a contractual remedy that could include clawback of funding or restitution.

## 6. Successor liability

Companies acquire a number of liabilities when they merge with or acquire another company, including those arising from contracts, torts, regulations and statutes. Successor liability is an integral component of corporate law and, among other things, prevents companies from avoiding liability by reorganising. What is often challenging, however, is determining whether the type of transaction through which one company acquired part or all of another company's shares or assets renders the acquired company a "successor". Typically, an acquiring company will acquire a target company by one of the three transaction structures: a share purchase,

[104] 12 U.S. Code § 1467a(a)(2).

[105] FAR, Section 9.403.

[106] Council of the European Union, *Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy-new elements* (2013).

a merger or an asset purchase.[107] Very broadly speaking, in a share-purchase structure, the acquiring company purchases all, or at least a controlling interest in, the target company's voting shares directly from the target's shareholders, which means that the target company will become the acquiring company's subsidiary, with the acquiring company effectively acquiring the target's assets and liabilities.[108] In a merger, two companies combine to produce a single entity, with the surviving company becoming legally responsible for all liabilities of the constituent organisations.[109] The successor liability analysis, however, becomes more complicated in the asset purchase structure, where the acquiring entity can selectively choose which assets and which, if any, liabilities it wants to acquire and where, consequently, it is more difficult to establish whether the acquiring entity should be considered the target's "successor".

MDBs' sanctions framework does not provide a definition of "successor" and this was at the core of a recent WB Sanctions Board case, in which the Sanctions Board had to determine whether WB had committed an abuse of discretion in determining (in its previous decision) that the appellant entity was a successor to a sanctioned entity. The Sanctions Board found that WB did, in fact, commit an abuse of discretion in making that determination.[110]

In reaching this conclusion, the Sanctions Board sought guidance from the WB's Legal Department on the definition of "successor", which advised that the WB's approach to successorship was based on a concept of economic successorship–specifically, whether the entity in question continues to carry out business operations of the sanctioned entity. [111] To that end, the Sanctions Board considered the following factors: common business lines and business address, ownership and managerial connections, corporate relationship, assignment of legal and financial rights and public understanding (which included consulting the government of the appellant's domicile on their views as to whether the appellant is indeed the sanctioned company's successor).[112]

Clearly, MDBs would benefit from further guidance on successor liability. The Sections that follow consider successor liability rules in the US and the UK, and make recommendations for further guidance under the Principles in order to provide greater clarity

## 6.1. US law

The FCPA Resource Guide says that "[a]s a general legal matter, when a company merges or acquires another company, the successor company assumes the predecessor company's liabilities".[113] Successor liability does not, however, create liability where none existed before: If, for example, an issuer were to acquire a foreign company that was not previously subject to the FCPA's jurisdiction, the mere acquisition of that foreign company would not retroactively create FCPA liability for the acquiring issuer.[114]

Despite this rule, however, an acquirer may try to avoid seller's liabilities by structuring the acquisition as an asset purchase. Under both New York law and traditional common law, a company that purchases the assets of another company is generally **not** liable for the seller's liabilities. The policy rationale for this rule is quite straightforward: First, it appeals to fundamental notions of fairness, according to which "[n]o person should be bound by contractual obligations that they have not voluntarily assumed".[115] Second, it increases certainty in the market-place and recognises the importance of the free alienability of property; an alternative broad rule of successor liability would have a "chilling effect on potential purchasers who might acquire the assets of a foreclosed business and find themselves liable for debts they never intended to assume".[116] However, there are four exceptions, and a buyer of a company's assets will be liable as its successor if: (1) it expressly or impliedly assumed the predecessor's tort liability, (2) the transaction is entered into fraudulently to escape such obligation, (3) there was a consolidation or merger of seller and purchaser, or (4) the purchasing company was a mere continuation of the selling company.[117]

The first and second exceptions are straightforward: When an asset purchase agreement provides that the acquirer will assume certain liabilities, the acquirer will be responsible for them. Similarly, when a company fraudulently transfers its assets to avoid its liabilities, courts will ignore the transaction and hold the successor responsible for the company's liabilities.[118] The "de facto merger" and the "mere continuation" exceptions are closely related. The formulations vary slightly by jurisdiction–for example, Delaware requires a transfer of all of the transferor's assets and an assumption of all of its liabilities, in exchange for a payment made in the shares of the transferee directly.[119] Broadly speaking, however, these formulations typically involve

[107] Matheson, *Successor Liability* (2011), at 374.

[108] Ibid., at 376.

[109] Ibid., at 377-379.

[110] WB Sanctions Board Decision No. 101 (December 2017).

[111] Ibid., at 4.

[112] Ibid., at 4-7.

[113] Criminal Division of the US Department of Justice and the Enforcement Division of the US Securities and Exchange Commission, supra note 28, at 28.

[114] Ibid.

[115] Matheson, supra note 107, at 381.

[116] *Glentel, Inc. v Wireless Ventures*, LLC 362 F. Supp. 2d 992 (N.D. Ind. 2005), at 1003.

[117] See, e.g., *Excel Energy, Inc. v. Cannelton Sales Co.*, 337 Fed. App. 480 (6th Cir. 2009), at 16.

[118] Philips, *The Federal Common Law of Successor Liability and the Foreign Corrupt Practices Act*, vol 6, (2016), at 103.

[119] Ibid., at 24.

elements or factors similar to the following: (1) continuity of shareholders and ownership, management, personnel, physical location and business operations; (2) whether sufficient consideration was given, particularly whether shares were given in exchange; (3) whether the predecessor ceased business operations and was dissolved shortly after the new company was formed; (4) whether the successor company paid any outstanding debts on behalf of the previous company in order to continue business without interruption; (5) the acquirer's intent or purpose when the new company was formed; and (6) whether the successor held itself out to the public as a continuation of the previous company.[120] These factors embody a policy that companies should not be able to avoid liability by simply changing their form or name and critically, both require continuity of ownership between the seller and the purchaser.[121]

In addition to the four traditional exceptions, some US courts have recognised other exceptions, such as a "continuity of enterprise" exception, which makes liability easier to achieve than the "mere continuation" exception, because it considers whether there was a continuation of the seller's *business operations* (rather than a continuation of ownership).[122]

Commentators have suggested that the "patchwork system of successor liability" has left asset purchasers guessing at judicial outcomes due to inconsistent and conflicting rules.[123] One of the proposed solutions is for a sale of substantially all of the assets to impose automatic liability on the acquiring company for the full extent of the seller's liabilities.[124] That way, the acquiring company would avoid potential liability under piece-meal theories of successor liability and would have certainty over which liabilities will stay and which will attach.[125] Notably, there does not exist a clear standard on when a "substantially all" threshold has been met. For example, in *Katz v. Bregman*, the Delaware Chancery Court held that a sale of assets that constituted 51% of the company's total assets and generated about 45% of the net sales constituted the sale of substantially all assets.[126] By contrast, in *Hollinger Inc. v. Hollinger International Inc.*, the same court concluded that a sale of less than 60% did not meet the "substantially all" threshold, if the remaining assets were "quantitatively vital economic assets".[127]

While there is no clear arithmetic test for determining how much is "substantially all", the author believes that the "substantially all" threshold should be determined on a case-by-case basis, by assessing, first, whether the asset in question constitutes most of the company's assets and, even if the asset represents a small percentage of the company's total assets, whether the sale will affect the company's ability to carry out its corporate purpose.

### 6.2. UK law

As in the US, in the UK, share acquisitions result in all assets and liabilities of the target company remaining with the target. Unlike in the US, however, in the UK an asset purchase can effectively insulate the acquirer from liabilities it does not expressly assume, except with respect to employees. Therefore, case law on successor liability in the UK asset acquisition context is sparse.[128]

Moreover, the SFO does not publish the equivalent of the DOJ/SEC FCPA Resource Guide and there is no formal guidance from the SFO or the Ministry of Justice on successor liability. Nevertheless, the UK Bribery Act offence for failing to prevent bribery subjects a company to strict liability where an "associated person" commits a bribery offense,[129] where "associated person" means a person who performs services for or on behalf of the company.[130] Consequently, an acquiring company that does not implement an adequate compliance programme may find itself responsible for continuing misconduct of the target company even where it was unaware of its occurrence.

### 6.3. Application of the foregoing principles to MDBs' sanctions procedures

From the above analysis, it appears clear that in share acquisitions, the successor assumes all liabilities of the target company. Similarly, in the case of asset acquisitions, it would seem natural for the acquirer to be responsible for any liabilities it may have voluntarily assumed, as well as in the case where a company fraudulently transfers its assets. It is less clear, however, whether MDBs should adopt the "de facto merger" and the mere continuation exceptions by analysing such factors as common business lines and business address, ownership and managerial connections and corporate relationship, as the WB Sanctions Board did.[131] As described above, this is based on a "patchwork system of successor liability" of US courts, all of which seem to apply different criteria in their determinations. Consequently, such analysis runs the risk of inconsistent and conflicting outcomes.

Instead, MDBs could adopt a more uniform approach with a sale of substantially all of the assets resulting in automatic liability on the acquiring company for the full extent

[120] Phillips, *The Federal Common Law of Successor Liability and the Foreign Corrupt Practices Act*, vol 96, (2015), at 104.

[121] Ibid.

[122] See, e.g., *Turner v Bituminous Casualty Co.*, 244 N.W. Second 873 (1976), at 878 and *Savage Arms, Inc. v Western Auto Supply Co.*, 18 P.3d 49 (2001), at 55-58.

[123] Matheson, supra note 107, at 399.

[124] Ibid., at 415.

[125] Ibid.

[126] *Katz v. Bregman*, 431 A.2d 1274 (Del.Ch.1981).

[127] *Hollinger Inc. v Hollinger International Inc.*, 858 A.2d 342 (Del. Ch. 2004).

[128] See Levy, Kutner, Miller and Scargill, *Private Mergers and Acquisitions in the UK (England and Wales): Overview*, (November 2017).

[129] UK Bribery Act 2010, Section 7.

[130] Ibid., Section 8.

[131] WB Sanctions Board Decision No. 101 (December 2017).

of the seller's liabilities. That way, the acquiring company would avoid potential liability under piece-meal theories of successor liability and would have some certainty over which liabilities will stay and which will attach. The "substantially all" threshold should be determined on a case-by-case basis, by assessing, first, whether the asset in question constitutes most of the company's assets and, even if the asset represents a small percentage of the company's total assets, whether the sale will affect the company's ability to carry out its corporate purpose.

## 7. Conclusion

The preceding sections have analysed the treatment of corporate groups by examining analogous provisions in the US and the UK legislation, including the EU sanctions and have proposed improvements to the Principles. Specifically, MDBs' sanctions regimes would benefit from greater clarity regarding a company's liability for sanctionable practices committed by its employees. Such liability should start off with strict liability, while rewarding companies–through the use of mitigating factors–for measurable actions to prevent the occurrence of sanctionble practices, as well as for voluntarily self-reporting and cooperating with the investigation. Only where a company could show that there was no failure to supervise and that appropriate measures were taken as soon as the wrongdoing was discovered, could this lead to further mitigating factors and possibly even provide grounds for exculpation. Such measures would also need to be accompanied by self-reporting and cooperation with the investigation. Moreover, MDBs would also benefit from further guidance on how to determine whether a company's compliance system was adequately designed and implemented and the FCPA Resource Guide could provide useful guidance in that respect.

Further, as regards a company's liability for sanctionable practices committed by its subsidiaries, MDBs' sanctions regimes should go beyond the current "wilful blindness" and "failure to supervise" principles, which are quite vague and instead should distinguish between the parent's culpability based on the actual knowledge and deliberate participation in the wrongdoing, on the one hand and organisational responsibility, on the other hand, which may arise from a failure to supervise or maintain adequate controls or ethical culture within the corporate group. Unlike actual knowledge and deliberate participation, mere responsibility should not normally lead to debarment, but instead to conditional non-debarment, where the parent company would be required to develop and implement effective anti-corruption compliance systems as a condition of non-debarment. Just as in the case of its liability for the misconduct of its employees, a parent company should also be rewarded–through the use of mitigating factors–for measurable actions to prevent the occurrence of sanctionable practices.

Additionally, as regards a company's liability for sanctionable practices committed by its parent company, MDBs' regime should be premised on the definition of "control", based on the actual control and not only a threshold share ownership, which typifies the rather simplistic OFAC approach. Such actual control can be ascertained by considering the indicia from the Regulation 960–from the parent company's right to appoint or remove a majority of the management or supervisory board members to having the right to exercise a dominant influence over the subsidiary pursuant to an agreement, rather the mere shareholding percentage.

Moreover, as regards successor liability, the Principles' presumption that sanctions should be applied to successors and assigns should be supplemented with guidelines for determining whether a company is a sanctioned party's successor or assign. Such guidelines should stipulate that a share acquisition should result in the assumption of liabilities by the acquirer, while an asset acquisition should result in the assumption of liabilities by the acquirer with respect to the liabilities it voluntarily assumed, where the asset transfer was fraudulent or where the acquirer purchased substantially all assets of the target. The "substantially all" threshold should be determined on a case-by-case basis, by assessing, first, whether the asset in question constitutes most of the company's assets and, even if the asset represents a small percentage of the company's total assets, whether the sale will affect the company's ability to carry out its corporate purpose.

Finally, sanctioning discrete business operations of the originally sanctioned entity is probably most meaningful in the context of settlement negotiations, where the respondent is fully cooperating with the investigators and may be expected to comply with the terms of the settlement agreement. For example, if a company's construction unit were to engage in a sanctionable practice, an MDB could negotiate a settlement with the company, such that the construction unit is debarred, but other company units in unrelated areas may still be eligible to benefit from the MDB-financed contracts. Inevitably, this type of arrangement would seem appropriate under exceptional circumstances–for instance, if a respondent company proved that the relevant unit acted against the company's policies.

# The Roles of Arrangers and Agents in Syndicated Lending Transactions: **Duties, Risks, Liabilities and Protections**

*Rafal Zakrzewski**

**Abstract:** In this article Rafal Zakrzewski focuses on the roles of arrangers and agents in syndicated lending transactions, particularly where such transactions are entered into on the Loan Market Association's recommended forms. The potential liabilities of arrangers and agents in contract, tort and for breach of fiduciary duty are weighed against the protective provisions in loan documentation that may preclude such claims. In other words, this article considers the scope for a lender to sue an arranger or agent to recover losses that the lender suffers in respect of an unsuccessful lending transaction. The discussion is structured around two High Court cases: ***Golden Belt 1 Sukuk Co BSC(c) v BNP Paribas*** in respect of arrangers' liabilities and ***Torre Asset Funding v RBS*** in respect of the liabilities of agents. Valuable lessons both for lenders who are members of syndicates, and for arrangers and agents themselves, can be drawn from these decisions. The article is concerned solely with matters of English law.

*Dr Rafal Zakrzewski is a solicitor (admitted in Australia in 1999 and in England & Wales in 2003) specialising in English finance, corporate and commercial law. He is a partner based in Baker McKenzie's Warsaw office and recently worked at the European Bank for Reconstruction and Development as a Senior Counsel and Associate Director. He holds a doctorate from the University of Oxford and has taught there and at the University of Cambridge. Rafal is an editor of *McKnight, Paterson & Zakrzewski on the Law of International Finance* (2nd edn OUP Oxford 2017) and has authored a number of other books on English private law. His latest work *McKnight & Zakrzewski on the Law of Loan Agreements and Syndicated Lending* was published by Oxford University Press in February 2019. Email: rafal.zakrzewski@bakermckenzie.com

## 1. Introduction

The purpose of this article is to examine briefly the roles of arrangers and agents in syndicated lending transactions. It will do so through the prism of two relatively recent English High Court cases which bring to life the scope of potential liability that an arranger or agent may be exposed to. They also provide the context for discussing the relevant provisions of Loan Market Association (LMA) recommended form documentation. An examination of these cases is instructive because it reveals the extent to which a lender who is part of a syndicate may rely on an arranger or agent, and conversely the extent to which a lender is left to act to protect its own interests. In short, this article addresses the question that may be posed by a lender who finds that it is unable to recover its loan from the borrower: when can I sue the arranger or agent? In answering this question, a number of matters need to be considered. First, the roles of an arranger and an agent have to be outlined. Secondly, the obligations and rights of arrangers and agents under LMA documentation need to be investigated. Thirdly, the protections that are included for the benefit of arrangers and agents in LMA documentation need to be examined. This article will first discuss the position of arrangers in the context of the recent case *Golden Belt 1 Sukuk Co BSC(c) v BNP Paribas*. Thereafter, the position of agents will be considered in light of *Torre Asset Funding v RBS*, the leading case in that context. However, at the outset it will be helpful to summarise briefly the nature of a syndicated loan.

## 2. The Nature of a Syndicated Loan

A syndicated loan allows a group of lenders to lend funds to a borrower on common terms and in a greater amount than what a single lender would be willing or able to do on its own because of commercial or regulatory constraints. Each of the lenders agrees to lend up to its commitment on the same terms and subject to certain inter-creditor provisions. The lenders agree not to amend or waive most terms without majority lender consent, and certain other terms are subject

to all lender consent. For example, they generally agree not to demand early repayment unless approved by the majority lenders and to share on a pari passu basis if the borrower makes only partial payments. Each of these provisions could be regulated in a separate intercreditor agreement. Conceptually, a syndicated loan can be viewed as a number of bilateral loans advanced on the same terms which are bound together by an embedded inter-creditor agreement.

It is a core principle of syndicated lending that each lender is owed a separate and independent debt. If the borrower does not pay, each lender can sue to recover its own debt. On the other hand, each lender's obligations are several and limited to their maximum commitment. No lender accepts responsibility for the lenders and to share on a pari passu basis if the borrower makes only partial payments. Each of these provisions could be regulated in a separate intercreditor agreement. Conceptually, a syndicated loan can be viewed as a number of bilateral loans advanced on the same terms which are bound together by an embedded inter-creditor agreement.

It is a core principle of syndicated lending that each lender is owed a separate and independent debt. If the borrower does not pay, each lender can sue to recover its own debt. On the other hand, each lender's obligations are several and limited to their maximum commitment. No lender accepts responsibility for the liabilities of any other lenders or owes fiduciary duties towards the others. For this reason, the lenders are careful to make it clear that the syndicate does not constitute a partnership.

Such multiparty lending transactions inevitably give rise to some coordination problems, which can be resolved through the appointment of arrangers and agents. An arranger is the person responsible for coordinating the process of putting together the syndicate and the facility documentation. An agent, on the other hand, is the person who thereafter coordinates the operation and administration of the loan facility for the lenders. This entails collecting and paying over funds to the entitled parties, distributing information, running voting processes in respect of amendments and waivers (of undertakings, events of default and conditions precedent) and coordinating the exercise of rights vested in the syndicate (particularly the right to demand early repayment).

## 3. The Arranger: Role, Rights, Duties and Protections

### 3.1. Role of the Arranger

The arranger is the bank or financial institution that is commissioned by the borrower to arrange the syndicated loan. That is, to put the financing transaction together. This task includes finding the syndicate lenders, settling the common terms for the loans in a term sheet, negotiating the facility documentation, bringing the transaction to signing and perhaps leading a selling-down exercise whereby the syndicate is brought into the transaction through assignments and transfers of commitments and participations.

Initially, the borrower awards the arranger a mandate to conduct the transaction. This is usually done in the form of an LMA mandate letter (either underwritten or best efforts).[1] In summary, the arranger agrees to perform three functions. First, the arranger will assist the borrower in compiling an information memorandum containing financial and business information required to enable the potential syndicate members to assess and price the proposed transaction.[2] Secondly, the arranger agrees to use its best endeavors to approach prospective lenders and supply them with information relevant to their decision. If the mandate is underwritten, the arranger may undertake to provide all or part of the total facility if the other lenders cannot be found to take part in the syndicate. Thirdly, the arranger will work with external lawyers to prepare the facility documentation, in consultation with the lenders.

The arranger performs its role in two stages. The first stage covers the time until the prospective lenders commit in principle to participate in the transaction. During this stage, the arranger invites the lenders to participate and supplies the borrower's information to them. The second stage covers the period when the arranger is involved in the preparation and negotiation of the formal facility documentation. In the first stage, the arranger is performing a service for the borrower, rather than the lenders. In the second stage, the arranger can no longer be said to provide services only for the borrower. It will have appointed lawyers to advise it and prepare the facility documentation, and in negotiating the documentation it will be performing services for the benefit of the future finance parties.

The arranger's role was considered in detail in the recent case of *Marme v Natwest Markets Plc*.[3] The High Court concluded that when negotiating finance documentation, the arranger was not necessarily an agent of the syndicate. Accordingly an arranger did not have apparent authority to make representations on behalf of the proposed syndicate members, particularly on matters that the syndicate members would have no knowledge of.[4] In this case the arranger's role was only to act as a middleman or conduit for relaying information.

Where the syndicate is in place from the signing of the facility agreement— that is, when all the intended lending banks sign the original facility agreement— the arranger's role comes to an end on signing. Where a wider syndication takes place through trading after the initial loan documentation has been signed, the arranger's role ends once the full syndicate has been brought into the transaction. The arranger is a party to the facility agreement for the sole purpose of benefiting from the contractual protections that are included, such as indemnities and exclusion clauses.

[1] These phrases are used in this context to turn an absolute or strict liability obligation to provide finance into a less onerous one based on a standard of conduct. The meaning of each of these terms is discussed in detail in Paterson and Zakrzewski (ed), *McKnight, Paterson, & Zakrzewski on the Law of International Finance* (2nd edn, OUP Oxford 2017), at 9.3.2 or Zakrzewski and Fuller, *McKnight & Zakrzewski on the Law of Loan Agreements and Syndicated Lending* (OUP Oxford 2019), at 1.2.10.

[2] See *Raiffeisen Zentralbank Österreich AG v Royal Bank of Scotland PLC* [2010] EWHC 1392 (Comm), [92]–[93] where the court concluded that an information memorandum contains what the arranger considers relevant and consequently prospective lenders cannot assume that it is comprehensive and contains everything that is relevant to a decision to lend.

[3] [2019] EWHC 366 (Comm), [436]-[447].

[4] This case concerned alleged misrepresentations regarding EURIBOR manipulation by the arranger. The court held that the misrepresentations alleged to have been made by an arranger would have been outside the scope of even its apparent authority to represent the syndicate. Consequently, the syndicate members could not be held liable for them.

### 3.2. Legal Risks Faced by the Arranger

A borrower may attempt to sue the arranger for breach of contract for a breach of the mandate or may allege a breach of a wider tort-based duty, such as a duty to advise. However, such claims have rarely been successful.[5] First, the mandate is usually carefully drafted to ensure that it does not contain an overly strict commitment to procure a syndicated loan and is usually subject to various conditions that will protect the lender from such contractual claims. Secondly, the courts have been very reluctant to find that banks are under implied duties to advise or provide comprehensive information to their clients.[6] The general position is that a relationship between a bank and a commercial borrower is arm's length and not advisory.[7]

The arranger is also at risk of being sued by members of the syndicate who enter into what proves to be a loss-making transaction, whether they are original lenders or lenders who subsequently acquire participations in the secondary markets. It is unlikely that such a claim could be brought for breach of contract because, as noted above, the arranger does not actually undertake any contractual obligations to the lenders in the finance documentation. Instead, there may be some scope to sue the arranger in tort for negligence based on a breach of a duty of care owed to the lenders, misrepresentation[8] or deceit for losses caused by a false statement of fact. However, successful claims by lenders against arrangers are extremely rare because the courts have traditionally resisted imposing wide duties of care on arrangers towards lenders. Nevertheless, as will be discussed below, a duty of care may be imposed with respect to some specific tasks undertaken by the arranger or concerning some particular information or explanation that it supplies.

The second reason why successful claims have also been rare is that the disclaimers in the information memorandum and the LMA recommended form contractual protections in the facilities agreement will usually function to preclude most claims. They do so by preventing a duty of care from arising (for example by making it clear that the arranger is not providing advice and that it is not assuming responsibility for the truth of the information that it is passing on from the borrower)[9] or by denying that any representation is being made or relied on, or simply by directly disclaiming liability for any losses that are suffered.[10]

The overall effect is that lenders generally have no claim against the arranger for the information it provides on behalf of the borrower since each lender is treated as carrying out its own research and making its own credit decision. Yet it must be borne in mind that an arranger will always be liable for a claim in the tort of deceit for any knowingly false statement of fact it makes to the lenders.[11] In such a case it is not necessary to prove any intention to cheat or injure.[12] Contractual protections cannot protect a wrongdoer against a claim in deceit as "fraud unravels all" including carefully drafted exemption clauses.[13]

### 3.3. Golden Belt 1 Sukuk Co BSC(c) v BNP Paribas

A recent case provides a good illustration of a rare and successful negligence claim against an arranger. *Golden Belt 1 Sukuk Co BSC(c) v BNP Paribas*[14] shows that in particular circumstances an arranger may bear liability for aspects of a financing transaction, including to purchasers of participations in the secondary market. Although it was not a case involving a syndicated loan, but another financial instrument, it provides an illustration of the type of claims that lenders could consider bringing against the arranger of a loan transaction.

BNP Paribas acted as the arranger of an Islamic financing transaction known as a sukuk (which is equivalent to a bond issuance). Repayment was secured by a promissory note governed by the laws of Saudi Arabia which an individual had purportedly signed. There was a default under the financing transaction. Creditors were unable to enforce the promissory note security because the signatory had used a laser-printed signature, not a wet ink signature, rendering it unenforceable under Saudi law. Distressed debt funds who had purchased the sukuk certificates in the secondary market brought proceedings against the arranger alleging that it had failed to perform its duty to exercise reasonable care to ensure the proper execution of the promissory note in accordance with applicable local law requirements.

The High Court had to determine whether the arranger owed the lenders a duty of care in putting together the transaction to ensure the due execution of the transaction documents. In answering this question, it used three tests put forward by the English courts for the existence of a duty of care giving rise to liability for pure economic loss. The first test is whether the defendant voluntarily assumed responsibility to the claimant for what it did.[15] The second test is the "threefold" test which poses three questions: (a) whether the loss to the claimant was a reasonably foreseeable consequence

[5] See also A Zharikov, 'Liability of the Arranger of a Syndicated Loan: Methods of Protection' [2015] 9 LFMR 154-157.

[6] *Carney v NM Rothschild and Sons Ltd* [2018] EWHC 958 (Comm), [58].

[7] *Deslauriers & Anor v Guardian Asset Management Ltd (Trinidad and Tobago)* [2017] UKPC 34.

[8] Sections 2(1) and 2(2) of the Misrepresentation Act 1967. *IFE Fund SA v Goldman Sachs International* [2007] EWCA Civ 811 and *Raiffeisen Zentralbank Österreich AG v Royal Bank of Scotland PLC* [2010] EWHC 1392 (Comm) provide examples of misrepresentation claims against arrangers.

[9] *Raiffeisen Zentralbank Österreich AG v Royal Bank of Scotland PLC* [2010] EWHC 1392 (Comm), [94]-[95].

[10] Such disclaimers and exclusion clauses may be subject to a test of reasonableness where the Unfair Contract Terms Act 1977 and Section 3 of the Misrepresentation Act 1967 apply. However, English courts have generally upheld them as reasonable in commercial contracts between sophisticated business persons: *Watford Electronics Ltd v Sanderson CFL Ltd* [2001] EWCA Civ 317, [63]; *Raiffeisen Zentralbank Österreich AG v The Royal Bank of Scotland PLC* [2010] EWHC 1392 (Comm). See Zakrzewski, *International Finance* (2017), supra note 1, at 9.5.5 or Zakrzewski, *Loan Agreements* (2019), supra note 1, at 3.5.5 for a full discussion of the legislation.

[11] *Derry v Peek* (1889) 14 App Cas 337.

[12] *Foster v Charles* (1830) 7 Bing 105, 131 ER 40; Derry v Peek (1889) 14 App Cas 337 (HL) 374.

[13] *HIH Casualty and General Insurance Ltd v Chase Manhattan Bank* [2003] UKHL 6; [2003] 2 Lloyd's Rep 61, [15]–[16].

[14] [2017] EWHC 3182 (Comm).

[15] *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1964] AC 465; recently applied in *Playboy Club London Ltd and others v Banca Nazionale del Lavoro SPA* [2018] UKSC 43.

of the defendant's actions; (b) whether the relationship between them was of sufficient proximity (that is, sufficiently close as a matter of law); and (c) whether it was fair, just, and reasonable to impose a duty of care.[16] The third test is the "incremental" test to the effect that the law should develop new categories of negligence incrementally and by analogy with established categories.[17] The closer the case is to the facts of a previous case where a duty of care has been found to exist, the more willing the court will be, by use of the incremental test, to find a duty of care.

Once a duty of care is established it is necessary to determine its scope[18] and to adjudge whether it has been breached through a failure to exercise reasonable care. Finally, the claimant must show that it placed reasonable reliance on the defendant, that its losses were caused by the defendant's breach of duty and that the losses were not too remote (that is, that it was reasonably foreseeable at the time that the breach occurred).[19]

In the *Golden Belt* case, the court found that the creditors were dependent on the bank for the proper execution of the promissory note and had no means of checking whether the promissory note had been properly executed. The court concluded that the functions of an arranger "invariably include responsibility for arranging the execution of the transaction documents." Both the assumption of responsibility test and the threefold test were met. The court held that there was no principled reason why as a matter of policy the arranger should not owe such a duty to purchasers in the secondary market.

The arranger was held to have assumed responsibility to take reasonable care to ensure that the promissory note was properly executed. The arranger attempted to rely on a disclaimer in the offering circular, but the court held that it was not sufficient to exclude responsibility for the execution of documents. The legal opinions given by external counsel contained the standard assumptions that the signatures were genuine.

Damages were left to be assessed at a later hearing. The successful claimants might not actually recover substantial damages. Instead, they may only be entitled to compensatory damages that will put them into the position that they would have been in had the wet-ink signature been obtained and the promissory note been enforceable. Since the individual who had signed the note was bankrupt and residing in Saudi Arabia, the claimants might not have actually recovered much more even if they had the benefit of a valid promissory note.

As noted, in the *Golden Belt* case, the disclaimer contained in the offering circular was insufficient to protect the arranger. However, an arranger of a syndicated loan transaction entered into in the LMA recommended form is protected by a greater array of protective provisions. For example, the LMA's "Multicurrency Term and Revolving Facilities Agreement"[20] contains the following disclaimers which would have assisted the arranger. Clause 26.4 limits the arranger's role to the matters expressly set out in the finance documents.[21] Clause 26.8 excludes liability for the enforceability of finance documents. Additionally, under Clause 26.15(b) the lenders confirm that they are responsible for making their own assessment of the risks involved in a transaction, including the enforceability of the finance documents.[22] Consequently, in the context of a syndicated loan documented on the basis of the LMA form, the arranger is unlikely to be found to be liable for failing to ensure the due execution and enforceability of a security document.[23] This is an excellent reminder of the wide-ranging nature of the disclaimers in LMA recommended form documentation, such that lenders must satisfy themselves as to all aspects of the transaction, including the accuracy and completeness of information supplied on the borrower's behalf and the effectiveness and enforceability of the finance documents. The lenders cannot look to the arranger to bear liability if something goes awry in these areas.

## 4. The Agent: Role, Rights, Duties and Protections

### 4.1. Role of the Agent

The agent, or more fully the facility agent, coordinates the facility once it has been entered into by the borrower and the lenders. The agent's role begins on the signing of the facility agreement and continues until the conclusion of the transaction. The agent's role is crucial to the management and effective coordination of the arrangements between the lenders themselves as well as between them and the borrower. The facility agent may be assisted by other entities which perform specific roles. Most commonly, if the facility is secured, a separate security agent or security trustee may be appointed on behalf of the lenders.[24]

The agent may have been an arranger and will also usually be a lender, but the documentation will clearly distinguish the rights and obligations it has in its capacity as agent from those it may have in other capacities.[25]

[16] *Caparo Industries plc v Dickman* [1990] 2 AC 605; *His Royal Highness Okpabi v Royal Dutch Shell Plc* [2018] EWCA Civ 191.

[17] *Caparo Industries plc v Dickman* [1990] 2 AC 605.

[18] A duty of care could be framed either as a wide duty to advise or take care of the interests of the lenders or as a more limited duty with respect to particular information that it supplies to the lenders or other tasks that it might undertake on their behalf.

[19] See Zakrzewski, *International Finance* (2017), supra note 1, at 9.4 or Zakrzewski, *Loan Agreements* (2019), supra note 1, at 3.4.3 for a more detailed discussion of these requirements.

[20] Version LMA.MTR.09, 21 December 2018 (accessed 27 January 2019).

[21] It states "Except as specifically provided in the Finance Documents, the Arranger has no obligations of any kind to any other Party under or in connection with any Finance Document."

[22] It states "Neither the Agent nor the Arranger is responsible or liable for [. . .] the legality, validity, effectiveness, adequacy or enforceability of any Finance Document [. . .]".

[23] It states "[E]ach Lender confirms to the Agent and the Arranger that it has been, and will continue to be, solely responsible for making its own independent appraisal and investigation of all risks arising under or in connection with any Finance Document including but not limited to: [. . .] (b) the legality, validity, effectiveness, adequacy or enforceability of any Finance Document [...]".

[24] If the security agent is based in a jurisdiction that does not recognise trusts, a parallel debt structure would be used instead of a security trust. Under a parallel debt clause the borrower acknowledges a separate and additional debt owed by it to the security agent. This debt exists simultaneously (in parallel) with the debt owed by the borrower to the lenders and is equal to the amount owed by the borrower to the lenders at any time during the term of the loan. The parallel debt structure was upheld in *Law Debenture v Elektrim Finance* NV [2006] EWHC 1305 (Ch).

[25] *Torre Asset Funding v RBS* [2013] EWHC 2670 (Ch), [196]; *Landesbank Hessen-Thüringen Girozentrale and others v Bayerische Landesbank, London Branch and another* [2014] EWHC 1404 (Comm).

The agent is appointed by the lenders to act as their agent, and acts as the representative of the lenders in dealings with the borrower. Information that has to be transmitted by the borrower to the lenders will be given to the agent to be distributed to the lenders. Waiver or amendment requests that the borrower wishes to make as well as the notices it wishes to give will be delivered to the agent, who will then inform the lenders. Notices on behalf of the lenders will be given to the borrower by the agent. Payments are also routed through the agent. The lenders transfer their respective participations in the facility to the agent who then advances them to the borrower. Similarly, the borrower makes its payments of interest and principal to the agent who then divides them up and transmits them to the relevant lenders. In short, the agent is a conduit for both information and funds between the syndicate and the borrower.

At first glance, the agent seems to have a lot of discretion when acting on behalf of the lenders. However, significant limitations are imposed by the facility agreement. Certain specified actions cannot be taken by the agent without the consent of all or a majority of the lenders. The majority lenders may give binding instructions to the agent as to how it must exercise its vested rights and powers. On the other hand, to protect the agent, the agreement will also provide that the agent may first require security or an indemnity from the lenders if it is to carry out the instructions.

## 4.2. Legal Risks Faced by the Agent

Lenders, if unsatisfied with the manner in which the agent has performed its role, may attempt to bring claims against it for breach of contract, in tort or for breach of fiduciary duty.

Actions for breach of contract simply require non-performance of a contractual obligation (express or implied), and the key elements of an action in tort have already been discussed. Additionally, actions can be brought for breach of fiduciary duty. An ordinary agent who enters into contracts on behalf of its principal is subjected to a number of duties (so-called "fiduciary duties") which are ordinarily implied into the agent-principal relationship by the general principles of equity. An agent must act in good faith, must not make an unauthorized profit out of its position, and must not place itself in a position entailing a conflict of interests. These duties are far-ranging and the remedies for their breach can be draconian. However, as will be discussed shortly, these duties can be limited or excluded by contract.

The nature of the claims that may be asserted against the agent and the approach of the English Courts to such claims in the context of LMA documentation are well illustrated by the High Court case of *Torre Asset Funding v RBS*.

## 4.3. Torre Asset Funding v RBS

In *Torre Asset Funding v RBS*,[27] the claimant was a lender under a junior mezzanine tranche of a structured loan. RBS created the finance structure and took a number of roles including lender, shareholder and, in particular, agent at the junior mezzanine level. During July 2007, emails passed between the borrower and RBS including a business plan containing projections of poor future performance. They showed the borrower would soon have insufficient cash flow to service the most junior layers of interest, and discussed restructuring the transaction to capitalise these interest payments. The restructuring never occurred as another lender withheld its consent and the transaction collapsed soon after the onset of the financial crisis in 2008. The claimant asserted that RBS, in its capacity as agent, should have informed it of the July 2007 discussions because they constituted a restructuring event of default under the LMA form. The form provides that an event of default occurs when "[the Borrower] by reason of actual or anticipated financial difficulties, commences negotiations with one or more of its creditors with a view to rescheduling any of its indebtedness…." The claimant alleged that had it been informed of the event of default, it would then have sold its interest in the loans before the borrower became insolvent in 2008. Another relevant fact was that before the insolvency, RBS had wanted to secure the claimant's consent to the restructuring amendment. That is, to the capitalization of interest due to the claimant as junior lender so that the interest liability would not lead to a payment default. Unfortunately, the relevant person at RBS had given an inaccurate explanation to the claimant for why the consent was being sought. The person explained that the consent was to retain cash in the business to fund capital investments rather than to prevent a payment default.

### 4.3.1. The claim for breach of contract

The claimant's case based on breach of contract failed. The agent had not breached any contractual term of the facility agreement by omitting to inform the claimant of the July 2007 discussions, even though they constituted an insolvency event of default, or by failing to pass on the business plan.

The clause specifying that the agent's duties are mechanical and administrative in nature was given full effect by Sales J. The agent was only bound to pass on the notices and information within the scope of the relevant provisions of the transaction documentation. The agent did not have to pass on all information regarding the borrower, such as its financial projections and business plan, which came into the agent's possession.

Where there had not been any actual communication to the agent of a default, the agent was not under a duty to make any evaluation whether there had been such a default and was not required to inform the other lenders of circumstances that could amount to such an event. The agent was also under no obligation, express or implied, to chase the borrower to provide documentation which it was contractually obliged to provide to the lenders. Consequently, it was for the lenders themselves to complain to the borrower about such non-performance of the information obligations.

The court held that the duties of the agent were defined exhaustively by the express terms of the agreement between the parties. There was no scope for implying a term importing a wider duty to inform. The argument for implying a duty

[26] *Bristol & West Building Society v Mothew* [1998] Ch 1, 18.

[27] [2013] EWHC 2670 (Ch).

to inform failed on the English law "necessity" test for the implication of terms.[28]

#### 4.3.2. The claim for breach of fiduciary duty

Under the general law of agency, an agent is usually a fiduciary of its principal. As such, the agent must act in good faith, must not make an unauthorized profit out of its position, and must not place itself in a position involving a conflict of interests. However, in the *Torre* case, Sales J held that the facility agent was not under a duty under the general law of agency to inform the lenders of the restructuring event of default or to pass on the business plan. This was because, despite the default position, the rights and duties of the agent-principal relationship depended on the particular terms of the contract between them. In this case the agent did not owe any fiduciary duties as they and their consequences were expressly disclaimed in the detailed LMA recommended form agency clause. This clause expressly provides that the agent is not to be considered as acting in a fiduciary capacity towards the lenders or any other person.

#### 4.3.3. The claim in tort

The claim in tort nearly succeeded in the Torre case. In providing the inaccurate explanations to the claimant, the bank (here found to be acting as a lender, not as the agent) had breached a voluntarily assumed duty of care not to misrepresent negligently the reasons for seeking an amendment to the financing documents. Although the bank did not have an obligation to provide such information, in choosing to do so it assumed responsibility for the accuracy of the information and consequently came under a limited duty of care. The case illustrates the point that such a limited duty of care, to one or more of the lenders, may be assumed on the facts with respect to some specific task or some particular information.

However, the claim failed and it was held that the damages suffered by the claimant were outside the scope of the bank's duty of care. The duty of care only extended to loss that might be suffered as a result of giving the consent to the amendment that was sought. Since that amendment was never actually voted through, no such loss was suffered. The information was never provided for the claimant to assess whether it should retain or sell the loan, so it could not claim the losses resulting from a decision not to sell. Losses caused by such a decision were therefore outside of the scope of the duty of care that had been assumed. The real cause of the losses here was that the claimant had made a loan to a borrower who became unable to repay and whose assets were insufficient to cover its debts. In any event, the claim would also have failed on the facts because the claimants could not prove that they would have actually sold their loan participations if they had been provided with the relevant information at the relevant time.

## 5. Conclusion

The cases demonstrate that in the ordinary course of events it is very difficult to sue successfully and recover meaningful damages from an arranger or agent in respect of a syndicated loan transaction. Their duties are narrowly defined in the recommended form documentation, their contractual protections are very extensive, and it is difficult to prove that damage was caused by the arranger or agent rather than the lender's decision to lend to an uncreditworthy borrower. However, the cases that have been examined in this article also demonstrate that in certain circumstances the lenders may have some recourse against specific actions taken by the arrangers and agents. Lessons can be distilled for both sides. The lesson for arrangers and agents is to be careful about acting in any way that may lead to the imposition of additional duties over and above what is embedded in the documentation. The lesson for lenders is not to assume that they can rely on arrangers and agents to protect their interests. In these carefully and intricately constructed relationships, and despite the use of the concept of agency with its fiduciary overtones, when things do turn sour, the legal situation is better summed up by the four-century old adage "every man for himself" rather than the equally venerable "all for one and one for all."

[28] See *Marks and Spencer PLC v BNP Paribas Securities Services Trust Company (Jersey) Ltd* [2015] UKSC 72.

# Designing for Good: **Blockchain Technology and Human Rights**

*Marjolein Busstra**

**Abstract:** Many international development organisations are currently looking into blockchain technology as a potential booster of development and innovation. For instance, the World Bank is one of the many organisations that has established a dedicated blockchain lab. While there are numerous blockchain applications with potential social benefits, in order to ensure that blockchain technology actually delivers on its promise, it is essential to implement a "human rights by design" approach in the development of blockchain applications. This article intends to show that there are very real and concrete guidelines to be distilled from the international human rights canon, which could and should inform the design of any blockchain-based applications, especially those that are intended to benefit society at large. The article examines a number of human rights that are specifically relevant in the context of blockchain technology, such as non-discrimination, privacy and access to remedy. It also briefly touches on various accountability aspects, and discusses the human rights responsibilities of governments, private actors and international development organisations in the context of new technologies.

## 1. Introduction

Many international financial organisations are currently looking into blockchain technology as a potential booster of development and innovation. The World Bank, like many other organisations, has even dedicated an innovation lab to this technology.[1] There are indeed numerous interesting blockchain applications with potentially enormous social benefits. In order to ensure that blockchain technology actually delivers on this promise, however, it is essential to implement a "human rights by design" approach in the development of blockchain applications. This article intends to show that there are very real and concrete guidelines to be distilled from the international human rights canon, which could and should inform the design of any new blockchain technology, especially those applications that are intended to benefit societies at large. Moreover, the article zooms in on a number of human rights that are specifically relevant in the context of digital technologies: non-discrimination, privacy and access to remedy, and discusses their implications for blockchain applications. Finally, the article also briefly touches on accountability aspects, discussing the human rights responsibilities of governments, private actors and international organisations in the context of new technologies.

For reasons of expediency, this article does not go into detail on definitions or technical aspects. A basic knowledge of blockchain technology is assumed. Neither does it go into definitional questions regarding human rights. A broad and inclusive understanding of the term is employed, referring to the internationally agreed canon of human rights, as it is contained in a number of international and regional instruments, as well as in authoritative soft law norms such as the UN Guiding Principles for Business and Human Rights.[2]

* Marjolein Busstra, PhD is a legal counsel at the Netherlands Ministry of Foreign Affairs. She advises on matters related to human rights, cybersecurity and new technologies.

[1] Stanley, *End Poverty, Restore Trust: Worldbank Dives into Blockchain with Lab Launch* (28 June 2017).

[2] Much useful information can be found on the website of the Office of the High Commissioner of Human Rights on universal human rights instruments, the major regional human rights instruments and the UN Guiding Principles on Human Rights. See also the information on the Eur-Lex website on human rights and data protection in the EU.

## 2. Blockchain applications and their impact on human rights

According to blockchain enthusiasts, blockchain technology promises more transparency, more security and more efficiency. All good, so it would seem. Indeed, numerous applications come to mind that could have a positive effect on the human rights cause. By way of example:

(i) Blockchain's property of storing information in such a way that no one can alter or delete it afterwards can be very useful in countering corruption or irregularities in public services. For instance, elections by blockchain are arguably much harder to manipulate than paper ballots.

(ii) Blockchain technology offers a tamper-free and reliable way of tracking activities and entitlements or assets. This can be especially beneficial in countries with immature governance systems, acting as a catalyst for economic activity and growth. A much-cited example is a blockchain registry of land rights in countries where official registration of land ownership is unreliable or non-existent.[3] Community members can register their claims to land and the underlying documentation in a reliable and transparent way, which makes it more difficult to deny their rights and seize their property unlawfully.

(iii) The ability to share data quickly and securely could benefit human rights defenders, journalists and other persons investigating and reporting on human rights violations. For instance, the International Bar Association has recently launched an app that allows people to share information about human rights violations in a secure way.[4] Blockchain technology could take this a step further, by making it more difficult for human rights violators to interfere or change data once uploaded.

(iv) Cryptocurrencies based on blockchain technology offer opportunities in terms of financial inclusion, by giving access to financial services to people in countries with immature or inaccessible financial infrastructure. Small-scale farmers and entrepreneurs can get access to global cryptocurrency markets and acquire loans or insurance in order to boost their business. Poor communities could benefit from blockchain based cooperative insurance schemes against failing crops or disability.[5] With these and similar applications, blockchain technologies can contribute to the fight against poverty.[6]

(v) The transparency implied by blockchain technology creates interesting possibilities for opening up supply chains, helping businesses in carrying out the human rights due diligence that is required of them by the UN Guiding Principles on Business and Human Rights (UNGPs).[7] Blockchain technology makes it easier to accumulate and share reliable information about where products come from and which journey they make until they end up on the shelves or racks for consumers to buy. Such supply chain blockchains could further include data about, for instance, labour conditions, tax returns or environmental protection safeguards. In this way, businesses not only gain more insight into the human rights risks in their supply chain, but can also show to the public how they prevent or mitigate the materialisation of these risks, by storing information in the blockchain about the measures they have taken. Similar supply chain initiatives have been launched in the cobalt sector in the Democratic Republic of Congo and the fishing sector in the Pacific.[8]

Exciting as these possible applications may be, blockchain technology is not more than an instrument. It can equally engender unwanted or negative effects, or not deliver on its promise if used in the wrong way or by the wrong people. After all, the aforementioned applications all require some extent of reliable human input and verification in order to be effective. A blockchain application recording land property rights can only benefit people if they already have some form of evidence of ownership that is recognised by the blockchain. The chain cannot create land rights, only record them. This may be problematic for indigenous communities who do not have any legally valid title documents for land they own by tradition. Similarly, for supply chain blockchains to function, one needs not only data about the origin and location of the product, but also someone to check that the information added is actually true.

Even if blockchains function perfectly, they can still lead to unwanted outcomes. Commentators have pointed to the risk of loss of jobs caused by the elimination of intermediaries in supply chains and by increased automation of production processes. Another potential risk lies in the lack of control of authorities over certain types of blockchains. Levying taxes on blockchain applications may, for instance, prove to be difficult, which could undermine public finances and result in lower levels of public service or public investments. Not to mention the risk of abuse of blockchain applications by repressive regimes or criminal or terrorist organisations.

Therefore, despite the great potential that blockchain technology holds, it would be naïve to assume that it is automatically a force for the good. This is especially the case since so much about the possibilities and limitations of this new technology is still unclear. This is exactly why it is important

[3] This is for instance already happening in Ghana: see Mwanza, Wilkins, *African startups bet on blockchain to tackle land fraud* (16 February 2018); and also in Georgia: see Shin, *The First Government to Secure Land Titles on the Bitcoin Blockchain Expands Project* (7 February 2017).

[4] International Bar Association, *International Bar Association Launches Mobile App that Captures Verifiable Images to Aid Prosecution of Human Rights Atrocities*, (8 June 2015).

[5] See, e.g., the second use case mentioned in Chaix, *5 Ways Blockchain Can Boost Economic Development* (26 April 2019).

[6] Ministry of Foreign Affairs of Denmark, *Hack the future of development aid* (2017), at 12. For a much more elaborate exploration of potential financial applications of blockchain technology, see Scott, *How can cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?* (2016).

[7] Principle 17 of the UN Guiding Principles states that: "In order to identify, prevent, mitigate and account for how they address their adverse human rights impacts, business enterprises should carry out human rights due diligence. The process should include assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed."

[8] Clarke, *Dem. Rep. of Congo: Blockchain technology can help improve cobalt supply chain, say experts* (13 February 2018); Visser, Hanich, *Fiji: Blockchain technology joint project launched to address illegal fishing practices and human rights abuses in pacific islands tuna industry* (23 January 2018).

to discuss ethical and legal issues surrounding blockchain, now that the technology is still in its infant stage. Which brings us to the core question of this article: how should human rights regulate or condition the use of blockchain and related technologies?

## 3. Making blockchain technology human rights compliant

There is broad international consensus that human rights apply in the digital domain and that persons should have the same rights online as they have offline.[9] Hence, to the extent that blockchain technology is used by, or impacts the lives of, humans, the affected individuals should be able to assert their human rights and have them respected and protected in exactly the same way they can in the analogue or physical world. This not only raises questions as to how to translate human rights norms to the new technical realities introduced by blockchain, but also as to how to enforce rights in a blockchain context. Three major themes come up in this respect: access, privacy and remedy, each of which is described in continuation.

### 3.1. Access

As the development and use of blockchain technology takes flight, more and more services and benefits will become available, perhaps exclusively, in the form of this technology. This in turn will make it increasingly relevant for individuals to have access to these services or benefits. There may come a time that access to blockchain applications is deemed so fundamental that it merits a right in itself, in a comparable way to the right to internet access that is currently debated. Even in the absence of a self-standing right to access, human rights law has relevance for a number of issues related to access to blockchains.

First, the right to non-discrimination requires that access to blockchains be provided in a non-discriminatory manner. Individuals may not be excluded from a blockchain application or offered less favourable treatment because of their ethnicity, religion or sexual preference or other legally recognised discrimination grounds. Insofar as it entails a prohibition of *direct* discrimination, using prohibited grounds directly as selection criteria, this norm is quite straightforward. Fully permissionless blockchains, which allow anyone to participate and do not impose any conditions for entry, would appear to automatically comply with this norm. Even for regulated permissionless blockchains and permissioned blockchains,[10] the prohibition of using certain selection criteria should not be too complicated to comply with. One simply has to ensure that the software does not select according to ethnicity, sexual preference, religion or other relevant criteria. In this respect, it is noteworthy that the prohibition of discrimination does allow for the use of certain specified discrimination grounds as selection criteria, as long as there is a legitimate justification for using them. Factors such as gender or age are relevant in certain circumstances. Think of health checks for age-related illnesses or gender- specific diseases. Entities or persons claiming such legitimate use of a particular selection ground should be transparent about it and clearly explain how and why this ground is used, in order to allow for public scrutiny.

A more complicated issue arises with respect to the so-called prohibition of *indirect* discrimination, which is based on the reality that discrimination can occur even when no prohibited ground is used as a selection criterion, because of a disproportionately damaging effect on a protected group. For instance, in many countries ethnic minorities live in relatively poorer neighbourhoods. If an online shop charges more for delivery to the postcodes of such neighbourhoods, or if the government selects such postcodes in catchment areas for lower quality schools, the ethnic minority living there is disproportionately disadvantaged compared to the general population. Absent a reasonable justification for such disproportionate effect, it amounts to indirect discrimination. In the same vein, if a smart contract or algorithm in a blockchain application takes into account characteristics that are more or less connected to a particular minority group, it could, perhaps unintentionally, disproportionately filter out persons of that minority group and produce discriminatory results. The potentially discriminatory outcome of automated decision-making is a concern that is increasingly being highlighted by human rights experts.[11] With reason: various instances of bias have already been found in facial recognition software, internet search engines and other algorithmic applications.[12]

All of this calls for thorough research into potentially discriminatory effects of proposed designs of blockchain applications and commensurate adjustments. However, the problem with indirect discrimination is that it often cannot be predicted in advance and is only established afterwards, by discovering a disproportionate negative effect on a particular group of people. Self-learning algorithms seem particularly capable of producing unforeseen forms of disproportionate negative impact, as they are programmed to find and use correlations and causations that are not immediately obvious. Hence, blockchain applications using such algorithms and similar technologies should not exclusively be checked for potentially discriminatory effects at the design stage. The results produced by software should be continuously monitored and mechanisms should be put in place to undo or remedy potentially discriminatory results. Moreover, it is vital that persons from minority or other underprivileged groups be included in the design and development processes and in any future governance discussions on blockchain and related technologies. This is also why the open source working method should generally be preferred with regards to the further development of blockchain, as it maximises transparency and allows broad scrutiny, in particular by users that may otherwise be overlooked.

[9] UNHRC, *The promotion, protection and enjoyment of human rights on the Internet* (27 June 2016).

[10] Regulated permissionless blockchains allow any person to join, but do require those who want to join to comply with a set of rules or conditions, which are set by the designer. By contrast, unregulated permissionless blockchains allow simply anyone to join with no strings attached. Finally, permissioned blockchains are only open to a specified group of persons or organisations and also operate in accordance with a set of rules.

[11] *Council of Europe, Algorithms and human rights, study on the human rights aspect of automated data processing techniques and possible regulatory implications* (2017), at 26; UN Special Rapporteur on the right to privacy, *Report of the Special Rapporteur of the Human Rights Council on the right to privacy* (19 October 2017), at 15; Barocas, Selbst, Big Data's Disparate Impact (2016).

[12] Lohr, *New study reveals racial bias in facial recognition software* (15 February 2018); *Miller, When algorithms discriminate* (9 July 2015).

The argument also holds true at a country level. Blockchain has the ability to reduce the costs of transaction processes significantly, and as transaction costs generally tend to be higher in developing economies, these have relatively much higher profits to reap from a transition to blockchain technology than developed economies. It is essential to pay attention to these countries in blockchain trials or pilots and to include them in any future blockchain governance or regulation debates. Otherwise, there is a real risk that these countries will fail to reap the benefits of new technologies and end up lagging even further behind, thereby reinforcing global inequality.

Reasoning further along the lines of non-discrimination and access: the practice of digital profiling, which is likely to be used in many blockchain applications, for instance in those employing smart contracts or self-learning algorithms, poses a real concern. It entails recording patterns of behavior and making profiles of persons based on seemingly unconnected and unnoticed digital activities of individuals. This is problematic because the premise of the prohibition of discrimination is that persons are to be treated as individuals, not as categories.[13] There is also a problem from the privacy perspective, because more information about personal choices may be revealed and recorded than persons are aware of or even have consented to. In addition, digital profiling can undermine individuals' ability to freely make personal, autonomous choices that shape their identity, which is a core element of privacy. Simply stated: I may not mind that people see me going into an ice cream shop on a particular day, but I do mind if someone records each time I go into the ice cream shop, finds out I always go on Thursdays after the gym and subsequently offers me a discount for low-fat ice cream, as this is the type of ice-cream most popular with people going to the gym. There is a real risk that blockchain applications coupled with certain Artificial Intelligence (AI) technologies will distinguish between individuals based on perceived trends and correlations, without checking their real profile or giving them a real choice. As a result, individuals may feel treated unfairly on the basis of some profile that is based on their own or someone else's behavior: what if I prefer to get a discount on full-fat ice cream? Getting ice cream is of course trivial, but more important interests may be at stake.[14]

At the same time, digital applications cannot exist without making use of trends and profiles. Indeed, many applications using big data and self-learning algorithms greatly enhance the quality of life, by offering tailored healthcare or fitness solutions, helping people to work more efficiently or giving consumers personalised offers that can save them money. Therefore, using these types of technologies may not be problematic in and of itself, but it may become problematic when people are not aware of their presence and do not have a real choice as to whether they want to benefit from them or not. This calls for maximum transparency from providers of such applications about when and how they use them. Moreover, individuals should have the opportunity to choose whether they want to participate in the applications that use this type of profiling and they should be able to change or correct profiles made of them. In Europe, both the European Union and the Council of Europe have produced guidelines and even enacted legislation in this respect.[15]

Another issue that comes up in the context of non-discrimination is the question of whether vulnerable groups should get additional assistance in gaining access to certain blockchain applications. This is particularly relevant to blockchain-based services operated by governments, as they have the obligation to provide for special measures for certain vulnerable groups.[16] Just as governments must provide access to public buildings and infrastructure for persons with disabilities, arguably, they should also assist the digitally vulnerable groups in accessing blockchains offered by the government. Think of applications in the field of education or healthcare. If these are too complicated for certain social groups, the human rights to education and to health require that these groups be assisted in accessing them.

A final word about access, or rather about non-access. What if individuals do not wish to have access to a particular blockchain application? In other words: if a service or a benefit that hitherto was offered in a physical form is transposed to a blockchain application, do persons have a right to continue using the physical alternative? What if a person wants to continue to communicate with a company or government through post or telephone, instead of an application on their smartphone? Do human rights canons say anything about a right not to go digital?

Two lines of thought are relevant here: First, if the introduction of digital applications threatens to lower the previously existing level of protection of human rights in a particular state, there is an argument to be made that states should provide for an alternative.[17] For instance, if the state introduces tax returns through blockchain applications for smartphones, arguably the state should also continue to offer the option of tax returns through paper and mail for the group of people who do not have such phones or do not know how to operate them. This argument closely resembles the one of the need for special measures for vulnerable groups. More fundamentally, there is an argument to be made for the right not to go digital based on the right to

[13] See, e.g., the conclusion of Advocate General Jacobs in Case C-227/04 *Lindorfer v. Council* (ECJ 27 October 2005), at 59, where he describes discrimination as "the reliance on characteristics extrapolated from the class to the individual, as opposed to the use of characteristics which genuinely distinguish the individual from others and which may justify a difference in treatment".

[14] For a very enlightening, yet disconcerting, discussion of what a world governed by autonomously operating algorithms may look like, see Wright and De Filippi, *Decentralized blockchain technology and the rise of lex cryptographia* (2015), at 40-44.

[15] See articles 13(2)f, 14(2)g and 22(1) of the Council Regulation 2016/679 (EU) on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) (2016) OJ L 119. Read together, these articles recognise the right not to be subject to a decision based solely on automated processing and require that individuals be notified about: (1) the fact that their data is being used for profiling purposes and (2) the logic that is used in the profiling process. See also Council of Europe (Committee of Ministers), *Recommendation of the Committee of Ministers to member states on the protection of individuals with regards to automatic processing of personal data in the context of profiling* (23 November 2010).

[16] See, e.g., *CRPD, General comment (2018) on equality and non-discrimination (2018); CERD, General recommendation No. 32 The meaning and scope of special measures in the International Convention on the Elimination of All Forms Racial Discrimination (2009); CEDAW, General recommendation No. 25: Article 4, paragraph 1, of the Convention (temporary special measures)* (2004).

[17] At least in the field of economic, social and cultural rights, the UN Committee on Economic Social and Cultural Rights applies the doctrine of non-regression; see CESCR, *General comment No. 3: The nature of States parties' obligations (art. 2, para. 1, of the Covenant)* (1990).

privacy. This has to do with the fact that digital applications seem to necessarily involve some degree of digital tracing, which means that certain data about users is recorded and stored for at least some period of time. If the right to privacy is interpreted as including a right to remain anonymous or a right to be forgotten, this may mean that at least some essential or fundamental services have to be offered in a physical or analogous way, in addition to the digital application.[18] Both suggested lines of thought are open for debate. But it is an important debate to have, as more and more aspects of human life are usurped by the digital realm.

### 3.2. Privacy

The right to privacy carves out a personal space, in which individuals have the freedom to determine and develop their own identity, relationships, ambitions and choices. In addition, the right to privacy grants the individual the right to decide to which extent they share information about this personal space with others. Privacy is, in short, about identity and ownership of data concerning that identity. The right to privacy is not absolute, and it depends on the specific circumstances of a case whether an infringement of someone's privacy actually amounts to a violation of their right to privacy. Different legal texts give different names to the test that needs to be performed to establish a violation, but they are more or less comparable.[19] Interferences are required to be legitimate and proportionate, meaning that they should pursue a legitimate aim and the severity and nature of the interference should be proportionate to this aim. If an interference with a person's privacy complies with these conditions, it is not unlawful and qualifies as a legitimate limitation.

Even though it can be argued that blockchain applications can empower people and therefore contribute to their creation of their digital identity,[20] there are equally a number of concerns that deserve consideration.

First, there is the aforementioned problem of the impossibility of participating in blockchains on an anonymous basis: even if one takes on a pseudo-anonymity when participating in a blockchain, it is still technically possible to connect that pseudo-anonymity to a person or location. At least at this stage of technological development. That means not only that a person's actions on a blockchain are visible to all participants, but also that they can always be traced back to the person. As mentioned above, it is important to consider whether there are certain services that are so sensitive or essential that individuals should be offered the choice of a physical or analogous alternative. This would make sense, for instance, for democratic elections or referenda, where people should arguably still be given the option of a paper ballot instead of a digital vote. For voluntary blockchain applications that do not offer essential services, there seems to be less of a problem, as it is up to individuals themselves to decide whether they want to give up their anonymity for a particular application. People already do that all the time, by making use of social media networks, applications on their smartphones or internet search engines. That being said, one could wonder how much this argument is still valid in scenarios where blockchain is so omnipresent that not participating results in not being able to normally participate in society. It therefore seems important to keep looking for technical solutions that make anonymous participation in blockchains possible.

This is not to say that anonymisation is the holy grail. If anonymous participation in blockchain were to become possible, new dilemmas most certainly would come up. Governments have very valid reasons to consider anonymous participation in blockchains undesirable. Think of issues to do with taxation, national security or fighting crime. Taking measures to limit anonymous participation in blockchains for legitimate reasons is not necessarily problematic from the privacy viewpoint, as long as the conditions for legitimate limitations are respected. Indeed, as will be argued in continuation, it is even desirable that governments start thinking about regulating blockchains in such a way that the potential benefits are maximised and risks are minimised.

Coming back to the current state of affairs, where anonymous participation is not possible, it is essential from the privacy perspective that any access to personal data on blockchain applications be controlled and monitored.[21] This means that developers of blockchain applications that collect, store or use personal data have to carefully consider which persons have access to such data and to what extent. In line with the proportionality element of the legitimate limitation test for privacy interferences, access should only be permitted to the extent necessary. What is needed, therefore, is a clear regime with regards to access to personal data and a controlling mechanism to monitor whether this regime is adhered to in practice. This may, for instance, mean that access is provided to certain people on a temporary basis. Or perhaps it is possible to close down access to certain personal data after a particular date, working with offline cryptokeys that are destroyed after some time. The point is that attention needs to be given to finding ways that restrict access to personal data as much as possible.

The second problem that arises in the context of blockchain technology and privacy is that, at the current stage of technological development, blockchains do not allow for altering data once recorded, which could in some cases be problematic. Take a transgender person who wants to retroactively change references to their gender in official documentation. This is not possible in the blockchain context, where the option of altering or deleting data has been traded for more secure and transparent data sharing. Clearly, there is tension here between, on the one hand, the right to create and develop one's own public identity and, on the other hand, the important element of privacy which in some

[18] In the GDPR, the "right to be forgotten", which had been developed by the European Court of Justice, is described in article 17.

[19] Article 17 of the International Covenant on Civil and Political Rights prohibits unlawful or arbitrary interferences of privacy, while article 8 of the European Convention on Human Rights requires interferences to be "in accordance with the law" and "necessary in a democratic society."

[20] Ministry of Foreign Affairs of Denmark, supra note 6, at 7.

[21] See article 5 (b) of the GDPR, which states that personal data may only be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". For a definition of personal data, take for instance article 4 of the GDPR, which describes the concept as follows: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

jurisdictions has inspired the recognition of a right to be forgotten and a right to change personal data about oneself in public and private databases.[22]

A number of considerations are relevant here. First, the impossibility of changing or deleting data calls for very careful consideration of which personal data are stored in the blockchain in the first place. To the extent that individuals have a choice of whether to participate in a blockchain application, this is primarily their own responsibility. If, for instance, a blockchain application that rents out cars records locations and routes taken, a person using such blockchain arguably accepts that information about their whereabouts is being recorded and stored. However, the right to privacy requires that the application explicitly inform users about which data is recorded and ask for their consent, so that they have a real opportunity to reflect on privacy implications.[23]

Individual consent holds less value in situations where the choice not to participate is not a realistic option, for example where the only way to rent a car is through a blockchain application. Consequently, the responsibility for carefully considering which personal data is recorded in the blockchain cannot solely lie with individuals. It is essential that designers and developers of blockchain applications afford sufficient attention to this question and only record and store personal data that is actually needed for the smooth running of the application. They should actively look for ways to safeguard privacy from the very beginning of the design process – this is the so-called principle of *privacy by design*.[24]

This brings us to the second point: when it comes to recording and storing personal data, less is more. In the same way that the legitimate limitations test of the right to privacy requires that access to personal data be allowed only to the extent necessary, it also requires that only those pieces of personal data that are necessary for the smooth operation of the technology or application be recorded. This calls for an active search for ways to minimise the amount of personal data needed for an application. An interesting example is the development of the concept of zero knowledge proof, which allows applications to run on the basis of verifiable "yes" or "no" questions about individuals' personal situations. For instance, if a bank wants to know whether an applicant for a mortgage earns enough to be able to pay the monthly installment, a zero knowledge proof application allows checking whether the applicant earns more than a certain minimum amount without needing to know the applicant's exact salary. Thus, zero knowledge proof allows keeping the amount of personal information needed for transactions at a minimum level.

Third, the impossibility of deleting data once recorded means that it is essential to ensure that personal data submitted to a blockchain is accurate.[25] Safeguards must be put in place for the verification of personal data and the adjustment of incorrect or incomplete data, before the data is recorded in the blockchain. As a general rule, the final decision as to the accuracy of personal data lies with the person whom it concerns, in line with the principle that individuals have ownership over their own identity. Exceptions to this rule may be necessary where personal data reflect decisions or actions of others who have a stake in the accuracy of the data. Think of official registers of civil status or health statistics. In such cases, it is reasonable that the responsible authority has the ultimate say on the accuracy of data submitted, but individuals should at least have the option to review data concerning them and request alteration if they consider the data inaccurate.

This is closely related to the fourth and final consideration regarding the inability to alter or delete data: it makes it all the more important to keep looking for technical or legal ways to enhance individuals' ownership of personal data. In this respect there are some promising initiatives to create digital identities or digital passports for individuals, based on blockchain technology. The idea is to create blockchains of digital safes for storing personal data, the keys of which are held by individuals themselves.[26] In this way, individuals can create their own digital identity and decide who they want to give access to which particular aspects of that identity. From the privacy perspective, such solution is preferable over a solution where governments or private organisations provide for (centrally stored) digital passports or identities.

### 3.3. Remedy

As noted above, individuals have the same human rights online as they have offline. This means that states have to respect human rights when using digital technologies such as blockchain. It also means that states have the obligation to protect individuals against violations of their human rights in the digital world. Acting against cybercrime is as much of the government's task as is acting against home burglary or physical abuse.

The argument for the equation of online and offline rights should hold not only for human rights. If I rent a car through a blockchain-powered application, I expect to have the same level of consumer protection that I would have if I rented a car from a physical car rental agency. Seeing that human rights law requires that states provide access to an effective and accessible remedy for people whose human or other rights have been infringed, it can be argued that states have to make sure that all their citizens' rights are as well protected online as offline. States are therefore advised to scrutinise their laws and regulations for digital – or blockchain - compatibility and update these if necessary. It should not matter whether the infringement originates with a real person in the physical world or with a blockchain application.

To be true, this does call for some flexibility. Contrary to the digital world, law is essentially not binary. Indeed, a fundamental characteristic of law is that it recognises that

[22] For instance, articles 16 and 17 of the GDPR require that data processors offer individuals the opportunity to request to delete or alter information about them and that they delete data as soon as they no longer (legitimately) need it.

[23] See article 6(1)a of the GDPR, which provides that personal data may only be processed with the consent of the individual concerned.

[24] See article 25 of the GDPR, which lays down the principles of data protection by design and by default.

[25] See article 5(d) of the GDPR, which requires personal data to be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".

[26] Aitken, *Blockchain to the Rescue Creating a New Future for Digital Identities* (7 January 2018); Floyd, *Blockchain Could Make You—Not Equifax—the Owner of Your Data* (25 June 2019).

reality is unpredictable. This is why it employs open concepts such as "reasonableness", "proportionality" and "necessity", which make sure that all particularities of a specific case are taken into account. This is also why law generally allows for hardship clauses that allow exceptions in extraordinary circumstances. Such open terms require a human mind that is capable of considering and weighing all relevant circumstances.

As long as digital activities involve some extent of human input or control, it would seem that the law can regulate them, either directly or by proxy, through the regulation of the relevant human actor. It was after all not too difficult for legal systems to adapt to the reality of email and smartphones. Even activities on the internet, a complicated structure that cannot be tied to a specific location or actor, generally proved to be governable through the regulation of activities of internet providers and tech companies.[27]

Thus, in order for law to be able to regulate blockchains and other new technological applications, ideally these should be designed to involve some extent of human input or control, which can subsequently be regulated. This involves, for instance, making sensible use of oracles in the blockchain process, which can add data to the blockchain, check the operation of the blockchain and intervene if necessary. Think of a certification institute that can verify claims about labour conditions or environmental safeguards in local factories and whose authorisation is needed for recording the relevant data in a supply chain blockchain. Another option is to require that applications of blockchain technology be accompanied by legally valid (e-)written agreements, that spell out the various responsibilities and rights of the participants.[28] For instance, this would mean that if I wanted to rent a car through a blockchain rental application, I would have to sign a written rental contract with the provider of the car.

However workable and feasible these solutions seem at present, it is questionable whether they will suffice in the longer run. Technology that does not need any human input after being created already exists. Indeed, the very concept of a smart contract is that it runs on its own, executing predetermined outcomes when predetermined conditions are met. Self-learning and -thinking AI applications go even further, not producing predetermined outcomes yet without needing human input. How can such applications be expected or forced to respect legal norms? Furthermore, even if there is a person or a group of persons behind a blockchain or comparable application, it may be impossible to identify or locate them, which will make it very difficult to enforce legal norms against them. This is particularly the case with permissionless blockchains. There can be informal groups of dedicated users that de facto manage the blockchain, but they are most likely not organised to such extent that they can be held accountable for the functioning of the blockchain. The same goes for distributed autonomous organisations (DAOs). In order for these entities to be accountable under national laws, they would have to be recognised as legal persons. But this presupposes some sort of founding act by one or more natural persons in a particular legal jurisdiction, according to the rules of that jurisdiction, whereas DAOs can simply be created online by any person without adhering to any rules. In a scenario where a great deal of digital interaction takes place with no immediately identifiable human actors, expecting digital applications to adjust to the existing legal paradigm does not work. Neither does the denying of the legal effect to the transactions or actions on blockchains that do not comply with the current legal paradigm, as this would lead to unwanted levels of uncertainty and impunity, undermining the rule of law.

Therefore, in the longer run, new, innovative solutions are probably needed, focusing on adjusting the legal system to make it compatible with the realities of blockchain and related technologies. This is very much unchartered territory and calls for creative thinking. Perhaps a form of collective insurance can protect against damage caused by blockchain applications that do not have an identifiable owner or manager. Perhaps providers or other intermediaries that offer access to a blockchain should to some extent be vicariously liable for damage caused by the blockchains in their portfolio. Perhaps certain legal principles or rules can be translated into code language that can be used in the software of blockchain applications or in smart contracts.[29] Going further, perhaps some fundamental concepts of law need adjusting. Take for instance, one of the central concepts of civil law: property and ownership. It is conceivable that, at some point in time, with the advancement of the internet of things, persons will hardly "own" any objects any more, but will only use or share them. Instead of a right to property, will they rather need some form of right to access? This article does not purport to answer these and similar questions that need consideration, but simply points out that there is a great need for further research. Given the complexity and multifaceted nature of the matter, a multidisciplinary approach is necessary, involving lawyers, technical experts, policymakers, as well as private stakeholders. It is advisable to aim for a discussion involving as many different stakeholders as possible, in order to ensure inclusiveness and coherence.

### 3.4. Accountability

A final word on remedies, more particularly on who is liable for remedying violations of human rights. The primary bearers of this responsibility are states. They have to comply with human rights standards when making use of blockchain technology and they have to ensure that users of blockchain technology within their jurisdiction both respect human rights themselves and are protected against violations by others. Given the potentially far-reaching implications of blockchain technologies for societies, it is therefore essential that states take an active role in the debates surrounding these technologies and perhaps even take part in their design process. This needs to be done both at the national and the international level, as blockchain technology, like any digital technology, does not respect physical borders. However, states are not the only ones that have human rights

[27] Wright and De Filippi, supra note 14, at 49.

[28] For instance, this is suggested in the Institute of Business Ethics, *Business ethics and Artificial Intelligence* (2018), at 5.

[29] Wright and De Filippi, supra note 14, at 55, mention the so-called "nearest person-theory", which would imply liability of creators of blockchain applications for damage caused by the applications they created or vicarious liability of users of blockchain applications.

obligations; private actors, including tech companies, bear a responsibility as well, particularly given that blockchain and technology generally originate with the private sector. According to the UN Guiding Principles for Business and Human Rights, businesses have to carefully examine their planned activities and projects for potential human rights impacts and take measures to prevent or remedy any negative impacts.[30] It does not suffice to wait for government regulation or actions by the public: an active effort to comply with and advance human rights is required.[31] Quite rightly, some commentators have therefore called for a *human rights by design* approach, which means that human rights are taken into account at the earliest time, when blockchain technologies are being planned and conceived.[32] Moreover, developers of technological applications need to be as transparent as possible with regards to what they plan to make and how their products work, and they need to make an effort to explain this in a way that people from other disciplines can understand. Only then can a meaningful discussion take place with regards to how these technologies can benefit human rights rather than harm them.

As regards the responsibility of international organisations, even though human rights law *per se* may not be applicable to them and, depending on the statutes of the organisation, they may even have full immunity with regards to human rights obligations,[33] there is a growing sense that they have a responsibility to respect human rights[34] – both in their own dealings and procedures and in the partnerships they enter into and the projects they support. Indeed, especially international financial institutions have a unique leverage that they can use to strengthen respect for human rights by third actors. There is a strong moral case to be made for these organisations to ensure the respect for human rights in their own activities and their cooperation projects with other partners, even though the law may not strictly require it. This would arguably require a shift in thought and practice[35] and perhaps would also call for the broadening of the staff skillset to include expertise in human rights and corporate social responsibility. This would seem a challenge worth taking on, seeing the major benefits for both the societies these organisations intend to benefit and their own legitimacy and credibility as being forces for good.

## 4. Conclusion

Blockchain is both a gift and a threat from the human rights perspective. In order to ensure that the positive impact outweighs the negative, it is necessary for human rights to be taken into consideration from an early stage in the development and implementation process of blockchain applications, as well as in broader discussions on the governance of blockchain and related technologies. *Human rights by design* is a crucial principle, as many of the human rights issues identified in this article can only be tackled in the very early phase of a new application. The right to privacy is especially vulnerable in this context. This is because of the immutability of blockchain, whereby the data once submitted cannot be altered or deleted, which means that mistakes made with regards to personal data cannot be undone. In addition, this is also because the right to privacy requires informed consent by consumers with regards to personal data and there is a real risk that blockchain applications are so technically complex that they easily defy an average person's understanding.

Even though businesses and other private actors have the responsibility to respect human rights, they probably need encouragement from governments, especially where human rights-friendly solutions cost money. This means that states should actively participate in the debates and trials currently taking place and that they should act timely to make sure their national legislation and policies are ready for the digital age. They have to make choices that promote and reinforce human rights before the technical reality makes choices on their behalf.

International organisations, particularly international financial organisations, many of which are already experimenting with blockchain technology, arguably have an equally important role here. Many of these organisations have considerable leverage in terms of the funds that they offer, which they should use to encourage responsible and human rights compliant design and use of blockchain technology.

Finally, a closer look at the points made in this article suggests that many of them are not exclusively relevant for human rights. Rather, they stem from a more fundamental, general unease of the current legal paradigm, developed in an analogous context and with an essentially human focus, with the digital paradigm, which is binary in nature and applies a logical, mathematical reasoning. As blockchain technology enters the phase of autonomously operating smart contracts and autonomous organisations, this tension will only increase. Not all technologies are the same, however. For instance, there is a fundamental difference between permissioned blockchains and unregulated permissionless blockchains. As permissioned blockchains or regulated permissionless blockchains run by certain rules, they can more easily be regulated and forced to fit into current legal systems. Unregulated permissionless blockchains, however, pose some fundamental challenges in terms of governability and accountability that cannot easily be solved. They call for a multidisciplinary, multi-stakeholder debate about how to make sure that they live up to their revolutionary potential in a way that is consistent with human rights and the rule of law. Technological experts and lawyers have so far each operated more or less independently. The challenges outlined in this article make clear that this can no longer continue. Legal and technical experts need to team up in order to devise solutions that are technically feasible and respectful of human rights.

[30] See Principle 17 of the UN Guiding Principles on Business and Human Rights.

[31] This obligation is not (yet) legally binding at the international level, as the UN Guiding Principles constitute the so-called "soft law." However, discussions on an international legally binding instrument are ongoing and more and more states have been adopting national legislation regulating businesses' responsibility towards human rights.

[32] Allison-Hope, *Human rights by design* (17 February 2017).

[33] See for an interesting analysis of this 'accountability gap': Zagel, *International Organisations and Human Rights: The Role of the UN Covenants in Overcoming the Accountability Gap.*

[34] Ibid. See also UN Special Rapporteur on Extreme Poverty and Human Rights, *Extreme poverty and human rights* (2015) and Dowell-Jones, *Financial Institutions and Human Rights* (2013).

[35] See, e.g., Desierto, *Lingering Asymmetries in SDGs and Human Rights: How Accountable are International Financial Institutions in the International Accountability Network?* (22 Feburary 2019).

# Privacy, the Fallacy of Consent **and the Need to Regulate Social Media Platforms**

*Lorena Barrenechea Salazar**

**Abstract:** This article analyses current privacy regulations and argues that they are failing to adequately protect the individual right to privacy. While regulations vary among jurisdictions, they generally allow consent to legitimise any form of collection or use of personal data. Consent, however, is regulated in such way that it does not require individuals to understand or even read the privacy policies they are agreeing to. This way, contractual law validates any form of collection or use of personal data. Based on this consent, social media platforms have collected personal data of individuals to the point that they are able to predict and influence human behaviour. This unchecked power needs to be addressed in new regulations.

## 1. Introduction

In the last decade, the world has gone through an unprecedented social transformation: Traditional means of communication have been virtually replaced by social media platforms. At the same time, these platforms are shaping the way we think, influencing our mood, preferences, relationships and even the results of democratic elections. This significant impact has been subject to little to no regulation. The most relevant regulatory developments have focused on the protection of privacy, aiming to ensure that consumers provide an informed consent to the use of their personal data by social media platforms.

This article argues that current regulations applicable to social media platforms are flawed, for two main reasons. First, by deficiently regulating consent, privacy laws allow an artificial, uninformed consent to legitimise the unlimited gathering of personal data by social media platforms and its use for any purpose. Second, in the biggest concentration of power ever witnessed by human history, current regulations fail to tackle or even acknowledge how social media platforms are already able to predict and manipulate human behaviour, decisions and emotions. In their inability to catch-up with technological developments, Governments and regulators have failed to take action, leaving the shaping of human will to a handful of private entities.

Section 2 of this article briefly acknowledges the current role of social media platforms in society. Section 3 analyses data protection regulations and explains how they end up legitimising the unlimited tracking of individuals by social media platforms. Section 4 explains the use of personal data by social media platforms, the effects of this use on society, and upholds that the collection and use of personal data social media platforms should be regulated. Section 5 sums up the conclusions on these topics.

## 2. Background: The Role of Social Media Platforms in Society

Social media platforms[1] are now essential to the participation in democracy and society.[2] Democratic processes around the world in the last few years have been heavily influenced by information, advertisement and news shared on social media platforms. At the same time, these platforms have become one of the main channels used by individuals to be informed and communicate.

From a legal standpoint, there has been ample debate on whether social media platforms classify as broadcasters, public utilities, common carriers or as a special category.[3] Regardless of categorisation, these platforms manage and moderate the content displayed to billions of users worldwide, on a daily basis.

* Legal Counsel, IDB Invest. The views and opinions expressed in this article are those of the author and do not reflect an institutional position of IDB Invest.

[1] For the purposes of this article, 'social media platforms' refers to any internet-based application that hosts user-generated content and that facilitates the development of social networks by connecting individuals.

[2] Jack M Balkin, 'Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society' (2004) 79 NYU L Rev 1, 4-5.

[3] Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harv L Rev 1598, 1660-1661.

By the second quarter of 2019, Facebook held an approximate of 2.41 billion active users worldwide,[4] representing roughly one third of the world's population.[5] Other social media platforms kept a smaller but equally significant number of active users, with Instagram reaching an estimate of 1 billion individuals and LinkedIn, Twitter and Snapchat[6] around 300 million each.

Many of these platforms either are monopolies or have a clear dominant position in the market. For an individual user, Facebook is virtually impossible to replace by another platform, concentrating a wide variety of services including photo and video sharing, personalized news feed, private messaging, groups of interest, event planning and recommendations, a search engine, birthday reminder and a memories recap, among others. This, together with the number of users and an aggressive acquisition policy that leads to the absorption of any rising star offering similar or comparable features, makes the company's position unique in the market.[7] In addition, the platform is constantly expanding its array of services, with the most recent announcement being the launching of its own currency.[8]

With Facebook dominating the space of social interaction, other platforms hold an analogous dominant position in their respective field, such as LinkedIn on professional networking or YouTube for video sharing. This way, social media platforms accumulate immense power and influence over a significant portion of the world's population.

Collection of personal data relays in the centre of social media platform's business model. Personal data allows platforms to show each user personalized content, mainly for advertisement purposes.[9] According to Facebook's latest audited financial statements, substantially all their income derives from advertisement. In 2018 and for this company alone, these revenues added up to USD 55.8 billion.[10] Other platforms show similar patterns, allowing the personal data gathered from their users to target individuals with personalized advertisements and content.

This business model has led personal data to become one of the most valuable assets in the world, comparable to oil.[11] Personal data is the cornerstone for the creation of artificial intelligence (AI), machine learning and other new technologies.[12] In this context, it is necessary to analyse the relationship of social media platforms with their users and the way it which the collection and use of personal data should be approached by Governments and regulations.

## 3. Data Protection Regulations, Consent and the Use of Data by Social Media Platforms

Privacy and the protection of personal data are fundamental rights. Article 12 of the Universal Declaration of Human Rights protects individuals against any arbitrary interference on their privacy, family, home or correspondence, which shall be safeguarded by law. Likewise, Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union recognize the right of individuals to the respect of their private and family life, home and communications and mandate that personal data must be processed fairly, for specified purposes and on the basis of consent.

These fundamental rights have been subject to further regulation in most jurisdictions. The most notable effort in this regard up to date is the General Data Protection Regulation[13] (GDPR) of the European Union (EU), in force since May 2018. Most specialists and public authorities agree that GDPR sets up the highest standards provided so far regarding privacy protection, with severe restrictions for the processing of personal data and strict standards for the validation of consent.[14]

Notwithstanding, current privacy regulations are failing to protect individuals from the unauthorised collection and use of their personal data. On the contrary, they are legitimising the existence of a surveillance regime that was never permitted by a legal framework. Article 6(a) of GDPR allows

[4] J. Clement 'Number of Facebook Users Worldwide as of 2nd Quarter 2019' <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> accessed 27 August 2019.

[5] The world's population in 2019 is estimated by the United Nations in 7.7 billion (United Nations, Department of Economic and Social Affairs, 'World Population Prospects 2019 – Highlights' <https://population.un.org/wpp/Publications/Files/WPP2019_Highlights.pdf> accessed 10 September 2019).

[6] Kristi Kellog, 'The 7 Biggest Social Media Sites in 2019', <https://www.searchenginejournal.com/biggest-social-media-sites/308897/#close> accessed 15 September 2019.

[7] The most notable acquisitions on this framework were the acquisition of Whatsapp for US$ 19 billion and Instagram for US$ 1 billion (Steven Musil, 'Zuckerberg Offers Peek at Facebook's Acquisition Strategies' Cnet (18 January 2017) <https://www.cnet.com/news/zuckerberg-facebook-offers-peek-at-acquisition-strategies/> accessed 1 October 2019). However, in the context of this strategy, Facebook has acquired over 75 startups and generally has a policy to buy any company that could potentially compete with the platform (Erin Griffith, 'Will Facebook Kill All Future Facebooks?' Wired (25 October 2017) <https://www.wired.com/story/facebooks-aggressive-moves-on-startups-threaten-innovation/> accessed 10 October 2019.

[8] Kari Paul, 'Libra: Facebook Launches Cryptocurrency in Bid to Shake Up Global Finance' The Guardian (London 18 June 2019) <https://www.theguardian.com/technology/2019/jun/18/libra-facebook-cryptocurrency-new-digital-money-transactions> accessed 10 October 2019. In addition, Facebook recently launched a dating service, demonstrating its unlimited appetite for dominating every aspect of social interaction (Katie Paul, 'Facebook Launches Dating Service in United States' Reuters (San Francisco 5 September 2019) <https://www.reuters.com/article/us-facebook-dating/facebook-launches-dating-service-in-united-states-idUSKCN1VQ1UO> accessed 10 October 2019).

[9] The business model is clearly explained on Facebook's terms of service: "We don't charge you to use Facebook or the other products and services covered by these Terms. Instead, business and organizations pay us to show you ads for their products and services. By using our Products, you agree that we can show you ads that we think will be relevant to you and your interests. We use your personal data to help determine which ads to show you" (--, 'Terms of Service' <https://www.facebook.com/legal/terms> July 31, 2019 accessed 1 October 2019).

[10] --, 'Facebook's Annual Revenue from 2009 to 2018' <https://www.statista.com/statistics/268604/annual-revenue-of-facebook/> accessed 15 September 2019.

[11] --, 'The World's Most Valuable Resource is No Longer Oil, But Data', The Economist (London 6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 1 October 2019.

[12] Jathan Sadowski, 'Companies Are Making Money from our Personal Data – But at What Cost', The Guardian (London 16 August 2016) <https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon> accessed 1 October 2019.

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation).

[14] See, for example, the comments from the United Kingdom´s Information Commissioner's Office at: Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)' <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> accessed 28 July 2019; or the comparative analysis of the EU-US standards on privacy protection at: Paul M Schwartz, 'The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 Harv L Rev, 1966.

private entities to collect personal data without limitation, as long as the individual expresses consent.[15] GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[16] Even though the definition requires an 'informed' consent, GDRP's recitals also indicate that such consent can be granted by ticking into a box, on an online pop-up.[17] The term consent is mentioned 71 times in GDPR and unlimitedly allows private entities in the EU to process personal data of individuals.

In the United States of America (US), consumer online privacy is protected by the so-called "notice and choice" mechanism, which also requires individuals to make an informed decision and consent to the processing of their information.[18] While regulations vary among jurisdictions, they generally follow a similar approach aimed at ensuring that individuals legitimise the use of their personal data by providing their consent.

Now, in practice, consent-based regulations have only led to numerous pop-ups showing up whenever a user opens a webpage. In the meantime, only a minimum percentage of individuals ever read the terms and conditions or privacy policies they are consenting to. Statistics show how less than 5% of individuals even actually click on the links that allow them to read the terms and conditions they are theoretically subscribing to[19] and how even intending to read them is virtually impossible, as it would take hundreds of hours of an individual's time.[20] Considering all the information they gather, it is safe to assume that social media platforms are aware of these statistics and therefore know for a fact that the alleged consent granted by individuals is not real: If individuals don't even click on the links leading to the information, they have no possibility to be aware of what they are consenting to.

Even for a small amount of users who read privacy policies and terms and conditions, these are normally written in legal jargon that does not allow individuals to properly understand their content.[21] In addition, from a technical point of view, most individuals lack the knowledge and expertise to adequately assess the consequences of authorising the use of their personal data.[22] Studies show how the sole existence of a privacy policy leads individuals to falsely assume that their personal data is being adequately protected.[23] However, it means the exact opposite, as the consent to the privacy policy is precisely the act legitimising the unlimited and unrestricted processing and use of their information.

Facebook's terms of service, for example, require individuals to consent on granting the company a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate and create derivative works of any post or content shared on the platform.[24] Moreover, their privacy policy legitimises the company to collect and process information about an individual's location, messages, other interactions with groups or individuals (including its content, frequency and duration), information gathered from connected devices or unconnected devices located in the proximity, operations and behaviours performed on these devices, mouse movements, information about nearby networks, pictures taken, religious views, ethnical origin, purchases, financial transactions, payment details, billing and shipping information and contact details included on each transaction, among others.[25] Thus, personal data processed by the company is not limited to the posts that users voluntarily upload but extents to likes and preferences, login habits and tracking of places visited; whom we are with and how long we stay. Similar practices are also held by other social media platforms.[26]

Few people truly understand what platforms do with this information: It is not only that they use locations to take

[15] Article 6 (1)(b) to (f) of GDPR regulates other five scenarios in which private entities are allowed to collect personal data without requesting consent: When it is necessary for the performance of a contract, to comply with a legal obligation, to protect the vital interests of an individual, for the performance of a task carried out in the public interest or in the exercise of an official authority or when it is necessary for the purpose of the legitimate interest pursued by the controller of the information or by a third party.

[16] GDPR, article 4 (11).

[17] GDPR, recitals para 32.

[18] Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harv L Rev, 1880.

[19] There are multiple studies on this topic and while results vary, it is generally agreed that around 1%-5% read privacy policies. Some studies even suggest that privacy policies and terms and conditions are read by only 1 in a thousand individuals (Andy Greenberg and The Firewall, 'Who Reads The Fine Print Online', Forbes (New York 8 April 2010) <https://www.forbes.com/sites/firewall/2010/04/08/who-reads-the-fine-print-online-less-than-one-person-in-1000/#4366220f7017> accessed 10 October 2019). Many statistics on this topic are presented on Solove, supra note 18.

[20] Multiple studies show that the length of these policies makes reading impracticable by a regular individual. In the US, it has been estimated that a regular individual would take an approximate of 244 hours per year if it wished to read the privacy policies of every webpage it visited at least once a year, and 154 hours if it wished to skim read them with the same frequency (Aleecia M. McDonald & Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies'(2008) 4 ISJLP 560, 553-564). In the EU, a recent trial conducted by the Norwegian Consumer Council revealed that it takes over 31 hours of continual reading to go through the terms and conditions of the apps commonly found on a smartphone (--, 'Norway Consumer Body Stages Live App Terms Reading', BBC (25 May 2016) <https://www.bbc.com/news/world-europe-36378215> accessed 27 September 2019.

[21] Kristen Martin, 'Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online' (2015) J. Public Policy Mark. 34(2), 212-212. Even if this complexity issue has theoretically been tackled by GDPR on the principle of transparency, that requires companies to provide information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language", in practice this simplified language is still full of legal terms that can only be understood on their correct scope and dimension by legal professionals.

[22] Solove, supra note 18, at 1886.

[23] There are multiple studies on this regard, showing that, for example, 75% of Americans believe that, when a website has a privacy policy, it means the website will not share their information with third parties (Joseph Turow, Lauren Feldman & Kimberly Meltzer, 'Open to Exploitation: American Shoppers Online and Offline' (2005) Univ. of Pa., Annenberg Pub. Policy Ctr. 6, 3).

[24] --, 'Terms of Service' <https://www.facebook.com/legal/terms> July 31, 2019 accessed 1 October 2019.

[25] --, 'Data Policy' <https://www.facebook.com/privacy/explanation/> April 19, 2018 accessed 1 October 2019.

[26] See, for example, personal data collection practices by Google (Dylan Curran, 'Are Your Ready? Here Is All The Data Facebook and Google Have About You', The Guardian (London 20 March 2018) <https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy> accessed 10 October 2019) or LinkedIn (Helena U Vrabec, 'The Curious Flows of your LinkedIn Data' Leiden Law Blog (Leiden 15 June 2017) <https://leidenlawblog.nl/articles/the-curious-flows-of-your-linkedin-data> accessed 10 October 2019.

note of a preference of a certain coffee shop; they actually build a completely new profile of individuals that most users are unaware of. For example, when a user opts out Facebook's personalized advertisement (an option that is well hidden but that can be accessed after persistently navigating through the platform) it is possible to verify that, based on their activity, users are classified in categories such as "compulsive buyer", "superficial soccer fan", "lives away from family", "5% highest per capita income", "extremely liberal", "single mother" and many others, that are determined based on individual behaviour. These categories demonstrate how, further to collect data, Facebook is conducting the most extensive psychological study of human behaviour in history. There are no statistics on this specific topic, but it is doubtful that many individuals are aware of these categories or have actually consented to be classified in such or to be shown content based on this information.

The constant tracking of individual's real space movements and online activity has caused some authors to declare that privacy is dead.[27] This reality is a reflection of consumer disempowerment, as individuals have been cornered to accept privacy policies and terms and conditions for platforms and devices of daily usage in such way that it is nearly impossible to use a phone or navigate the internet without constantly revealing personal information, location, company and other sensitive details of individual daily activity.[28]

This tracking of our personal lives is allowed by law because people 'consent' it constantly, when they agree to the platform's privacy policies and terms and conditions regulating them. Contractual law then allows social media platforms to collect massive amounts of data worldwide. As these platforms continuously create and update their own regulations, traditional law is progressively replaced by rules established by private entities such as social media platforms. The law of the state is then substituted by private regimes,[29] which keep a great amount of discretion.[30]

Although advocates of self-regulation claim that private regimes will lead to the best possible set of rules, as individuals will naturally lean the balance towards the best regulated community,[31] if users do not even read terms and conditions or privacy policies this imaginary market for best practices does not really exist. Besides, this logic fails to consider that, with billions of active users, any alternative to the currently available social media platforms only exists as a theoretical exercise. Leaving a social media platform is difficult and means losing social connections and interactions.[32]

Individuals may not even have a choice on granting consent. As noted in Section 2, social media platforms dominate a variety of social interactions, with billions of active users worldwide. Professor Steven M. Bellovin, computer science expert at Columbia University, explains how it is almost unattainable to participate in modern life without spreading our personal data across devices and platforms: "if you can't live without it, is your consent voluntary?".[33] If individuals are not even able to understand what is being collected about them nor the secondary uses of such information, an informed consent is not even possible.[34]

## 4. The Need for an Increased Protection of Privacy and Personal Data

The model of privacy protection is flawed, particularly in the assumption that individuals make informed decisions.[35] The great value of personal data, in combination with the lack of transparency on the ways in which data is collected and used by social media platforms, creates a need for improved regulation above and beyond consumer's choices and claims for stronger and more active consumer protection authorities.[36]

While most authors reject any proposal for regulation claiming paternalism, it is unclear why these proposals generate such a wide rejection. Consumer protection regulations exist in any industry in which the asymmetry of power is such that it justifies the intervention of the Government for the protection of individual rights.

This is the case, for example, of public services such as water and electricity. Critiques claiming paternalism would argue that the reason why those markets are regulated is that they are essential for human living. Even if participation in social media platforms were not essential for individuals, the asymmetry of the parties involved in the contractual relationship would still entail enough merit on itself to justify the need for stronger regulation and supervision.[37]

The need for regulation of social media platforms can be compared to the necessity to regulate consumer transactions on the banking sector. Diverse legislation worldwide aims to guarantee that consent granted by individuals to banks is not limited to the signing of a form but involves an actual understanding of the terms and conditions of the transaction that they are agreeing to. In addition, most jurisdictions impose banks several limitations on the contractual terms of their relationship with consumers, establishing limits on interest rates, fees and charges, indebtedness, limits for

[27] Joshua AT Fairfield, 'Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life' (2012) 27 Berkeley Tech LJ 1, 103.

[28] Ibid., at 103-14.

[29] Margaret Jane Radin, 'Regulation by Contract, Regulation by Machine' (2004) 160 JITE 1, 143-146.

[30] Andrew Jankowich, 'EULAw: The Complex Web of Corporate Rule-Making in Virtual Worlds' 8 Tul J Tech & Intell Prop 1, 44-45.

[31] Klonick, supra note 3, at 1625-1630.

[32] Nicholas Suzor, 'The Role of the Rule of Law in Virtual Communities' (2010) 25 Berkeley Tech LJ 4, 1826.

[33] Steven M Bellovin, 'Unnoticed Consent' (2018) 16 IEEE Security & Privacy 9, 80-79.

[34] Ibid., at 80-79.

[35] Stefan Larsson, 'Algorithmic Governance and the Need for Consumer Empowerment in Data-Driven Markets' (2018) 7 Internet Policy Rev 2, 8.

[36] Stefan Larsson, 'Algorithmic Governance and the Need for Consumer Empowerment in Data-Driven Markets' (2018) 7 Internet Policy Rev 2, 8.

[37] The power of social media platforms is such that some authors suggest that they resemble a governor-citizen relationship rather than a producer-consumer one (Jack M. Balkin, 'Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds' (2004) 90 Virginia LR 8, 2093).

overdrafts and for the granting of guarantees, among many other restrictions.

In the meantime, banks are neither a monopoly nor a public service; individuals with a regular income are reasonably able to go through life without requesting any banking service, and if they voluntarily decide to do so, they normally have a number of financial institutions and services they can choose. Despite this, there is little to no debate on the convenience of protecting consumers in their relationship with banks; it is assumed that the asymmetry on the parties involved in the transaction justifies regulations aimed at protecting individuals. If anything, there is a constant tendency to increase the level of protection granted to consumers on banking and financial matters.

While some banking provisions could be inspiring to understand the kind of measures that would need to be implemented beyond the current consent regime governing privacy, regulation of social media platforms needs to be drafted considering their particular characteristics and background.

Specifically, data protection regulations should focus on mechanisms for guaranteeing the real consent of individuals for the collection and use of their personal data and regulate the use that private entities give to it.

Nowadays, social media platforms use this data in a variety of ways, mainly by targeting individuals with personalized content. While some authors argue that the main difference between these platforms and other means of communication is their openness, as they allow democratic participation and are not dominated by an exclusive few,[38] this standpoint misses out on the fact that social media platforms are in fact owned and governed by only a few private entities, which keep absolute dominion and discretion to decide what one third of the world´s population sees on their screens. Even if users do have the freedom to publish what they deem appropriate, the alleged democracy is lost when platforms moderate content, arbitrarily deciding what content each user is exposed to, on a clear threat to freedom of speech and democracy.[39] Thus, contrarily to allowing a democratic flow of information and equal participation, as the defendants argue, social media platforms ferociously limit freedom of speech of their users.

This moderation takes place with very little transparency on how the platforms decide what is displayed on the newsfeed of their users or the rules for this moderation.[40] In this context, as virtual and real worlds converge, regulations of the virtual world progressively take over to govern everyday life.[41] In the meantime, Governments and regulators fail to catch-up with the development of new technologies and these platforms continue to moderate content and control virtual interactions, governing society with no supervision and with an extraordinary unchecked power. By moderating and personalizing content, social media platforms have taken unprecedented control and an extraordinary ability to control what people think,[42] on a rising trend away from individual choices and a free market towards corporate control of consumers.[43]

In his book Life 3.0, AI expert Max Tegmark opens with a fictional scenario in which a tech company buys the media and starts subtly shaping the news in order to manipulate public opinion.[44] While this fictional scenario aims to imagine the future of AI, with social media platforms it becomes real already, with a handful of individuals controlling the thoughts and will of billions of persons. This is a massively underestimated and powerful force shaping the world that needs to be acknowledged by legislators.[45] Social media platforms know us better than we know ourselves and have the ability to manipulate our will.[46]

Just to provide an example, it is a widely accepted fact among experts that the results of the vote for the United Kingdom to exit the EU and the election of the current President of the US were shaped mainly by targeted advertisement ran through social media platforms. As explained by Brittany Kaiser, involved in the Cambridge Analytica case, the information available on each Facebook user allowed the company to identify undecided voters. Among those users, Cambridge Analytica selected those who would be easier to swing and on what specific triggers, and then targeted them with personalized advertisements.[47]

Although the case is known mainly for the illicit, unconsented transfer of personal data by Facebook to Cambridge Analytica, it is also alarming to see how the data collected by the social media platform combined with sophisticated technology was able to alter the result of a democratic process. Also, while the case has been subject to public rejection partly because the results achieved were unpopular, similar targeting and algorithmic technics were already applied years before by Barack Obama without any criticism, with the only difference that these other candidates utilized the data and hired the services from Facebook and other social media platforms directly. This means that, as it stands now, social media platforms are legitimised to decide on the

[38] Klonick, supra note 3, at 1618-1622.

[39] Jack M. Balkin, 'Old School/New School Speech Regulation' (2014) 127 Harv L Rev 8, 2300-2301.

[40] Lawrence Lessig, *Code 2.0* (2006) 4-5.

[41] Fairfield, supra note 27, at 107-108.

[42] Marc Zao-Sanders, 'How to Think for Yourself When Algorithms Control What you Read', Harvard Business Review (8 March 2018) <https://hbr.org/2018/03/how-to-think-for-yourself-when-algorithms-control-what-you-read?fbclid=IwAR1qzzF1bmI5tRoG48wBnVoZTeo1iFKU4M6uX9JSUQ4tZvlia60TZTrXL1Y> accessed 15 August 2019.

[43] Fairfield, supra note 27, at 93.

[44] Max Tegmark, *Life 3.0* (2017).

[45] Tristan Harris, 'Optimizing for Engagement: Understanding the Use of Pervasive Technology on Internet Platforms. Written Testimony to the Committee of Commerce, Science, and Transportation – Subcommittee on Communications, Technology, Innovation and the Internet of the United States Senate' (25 June 2019) <http://humanetech.com/wp-content/uploads/2019/06/Testimony-Background-Tristan-Harris_CHT.pdf> accessed 1 September 2019.

[46] Nicholas Thompson, Interview with Yuval Noah Harari, Historian, and Tristan Harris, President of the Center of Humane Technology (10 April 2018) <https://www.wired.com/story/artificial-intelligence-yuval-noah-harari-tristan-harris/> accessed 1 September 2019.

[47] Karim Amer & Jehane Noujaim, *The Great Hack* (2019).

results of any democratic process around the world, and we have allowed them to do so with our 'consent' on the use of our personal data.

Experts in technology account that techniques applied by these companies for the persuasion of humans are effective regardless of age, race, gender, educational level or intelligence quotient.[48] Some of them even claim that the effectiveness is such that they make "free and fair election(s) meaningless".[49] In an illustrative interview, Tristan Harris, former chief of ethics and human persuasion at Google, explains how our minds don't work the way we think and social media platforms are already able to hack human beings, understanding them, predicting them and manipulating them at their will. While most individuals do not like to admit that their will can be influenced, multiple studies show otherwise, demonstrating that our will is already being swayed by technological devices.[50]

To some experts, the ability of social media platforms to know, understand and manipulate human thoughts and preferences represents a technological and a philosophical crisis.[51] The Center for Humane Technology, founded by former tech-executives, is gathering studies that show how social media platforms are having severe negative effects in individuals in a wide array of aspects, such as attention deficit, mental health problems, loss of empathy and difficulties socializing, among others.[52] They claim that social media platforms are already able to predict whether an individual is lonely or suffering from low self-esteem, whether they are about to start a relationship and even to determine the individual's sexual orientation even before the person is aware of it itself.[53]

Whereas it is common for social media platforms to refuse to sell or share data for purposes they do not support (such as the use of AI for military purposes[54] or gun sales[55]), the authority for deciding what personal data can or cannot be used for should not rely on a handful of companies, but on Governments and regulators.

The capabilities of data driven technologies keep rising, in terms of both collection and processing of data and on the development of algorithms, profiling and targeting of information. This means that the power of social media platforms continues to grow and the asymmetry between platforms and individuals increases exponentially.

Content moderation can lead to polarized populations and the radicalization of points of view,[56] which may turn to violence and terrorism.[57] While the manipulation of users should be the main concern for the regulation of social media platforms, this data is being used in ways unknown to individuals in other fields. Data has recently been used by authorities to identify and deport illegal immigrants[58] and for defence and military purposes.[59] These practices can lead to the perpetration of biases and discrimination[60] as individuals are profiled by computers and then treated accordingly, sometimes with no human intervention. This happens also in other fields such as recruiting or credit access, in which private entities are progressively taking algorithm-based decisions based on personal data collected by social media platforms.

Although there is no doubt that personal data can be used for research purposes in benefit of the public, it is necessary to distinguish those cases from social media platforms and other service providers, who gather personal data only for the generation of private gain.[61]

The rule of law is a human good that aims to limit the exercise of power. Transformative communication technologies call for regulatory innovation.[62] Deficient prudential regulations on the banking sector lead to the financial crisis of 2008, with devastating consequences around the globe.[63] One of the factors originating the crisis was that individuals did not understand what they were consenting to and were subsequently unable to honour their financial obligations. In parallel, banking prudential regulations were deficient and failed to prevent the crisis.

---

[48] Ramesh Srinivasan, 'Yes, Google is Disrupting our Democracy. But not in the Way Trump Thinks' The Washington Post (Washington DC, 21 August 2019) <https://www.washingtonpost.com/opinions/2019/08/21/yes-google-is-disrupting-our-democracy-not-way-trump-thinks/?noredirect=on> accessed 22 August 2019.

[49] Philip Bump, 'Trump Stumbles onto a New Justification for Losing the Popular Vote: It's Google's Fault', The Washington Post (19 August 2019) <https://www.washingtonpost.com/politics/2019/08/19/trump-stumbles-onto-new-justification-losing-popular-vote-its-googles-fault/> accessed 22 August 2019.

[50] Nicholas Thompson, supra note 46.

[51] Ibid.

[52] Center for Humane Technology, 'Ledger of Harms' (14 December 2018) <https://ledger.humanetech.com/> accessed 1 September 2019.

[53] Harris, supra note 45, at 6.

[54] Drew Harwell, 'Google to Drop Pentagon AI Contract After Employee Objections to the 'Business of War'', The Washington Post (1 June 2018) <https://www.washingtonpost.com/news/the-switch/wp/2018/06/01/google-to-drop-pentagon-ai-contract-after-employees-called-it-the-business-of-war/> accessed 21 August 2019.

[55] Matt Drange, 'Inside The Secret Group for Gun Owners Banned from Facebook', Forbes (New York 3 May 2016) <https://www.forbes.com/sites/mattdrange/2016/05/03/as-facebook-struggles-to-combat-gun-sales-one-of-its-own-brings-gun-groups-back-online/#35ac958659e6> accessed 10 October 2019.

[56] European Parliament Research Service – Panel for the Future of Science and Technology, 'Polarisation and The Use of Technology in Political Campaigns and Communication', (Brussels March 2019) <http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf> accessed 10 October 2019.

[57] Rachel Kleinfeld, ''Privilege Violence: Why Polarized Democracies Yield Violence' (30 January 2017) <https://carnegieendowment.org/2017/01/30/privilege-violence-why-polarized-democracies-yield-violence-pub-67871> accessed 10 October 2019.

[58] Douglas MacMillan & Elizabeth Dwoskin, 'The War Inside Palantir: Data-Mining Firm's Ties to ICE under Attack by Employees' *The Washington Post* (22 August 2019) <https://www.washingtonpost.com/business/2019/08/22/war-inside-palantir-data-mining-firms-ties-ice-under-attack-by-employees/> accessed 1 September 2019.

[59] See, for example, Patrick Tucker 'The Military is Already Using Facebook to Track Your Mood', Defense One (2 July 2014) <https://www.defenseone.com/technology/2014/07/military-already-using-facebook-track-moods/87793/> accessed 1 September 2019.

[60] Alex Hern, 'Data Collection Leads to Discrimination and Self-Censorship, MPs told' The Guardian (16 June 2019) <https://www.theguardian.com/technology/2019/jun/19/data-collection-leads-to-discrimination-and-self-censorship-mps-told> accessed 1 September 2019.

[61] Paul Ohm, 'Response: The Underwhelming Benefits of Big Data', 161 U Penn L Rev 339 (2013), 346.

[62] Jonathan A Obar & Steven S Wildman, 'Social Media Definition and the Governance Challenge: An Introduction to the Special Issue', *SSRN Electronic Journal* (August 2015) <https://isidl.com/wp-content/uploads/2017/08/E4559-ISIDL.pdf> accessed 1 September 2019.

[63] Jeff Sovern, 'Fixing Customer Protection Laws So Borrowers Understand their Payment Obligations', 46 J of Cons Affairs (2014), 17.

Privacy has a major social impact,[64] it is a human good.[65] The collection and use of personal data by social media platforms and their moderation of the content shown to users' need to be regulated and supervised by public authorities before a new crisis arises.

Being an extremely complex matter, any proposal for regulation needs to arise as the result of a multidisciplinary effort that takes into account the legal, technological, economic, psychological, sociological and philosophical aspects of the phenomenon. The consent approach needs to be abandoned. Limits and prohibitions need to be imposed to the collection and use of personal data for the protection of the public interest, human dignity and fundamental rights.

## 5. Conclusion

Privacy regulations based on the premise of consent are overlooking abundant evidence showing that individuals do not read privacy policies and mostly do not have the technical expertise required to understand them. GDPR does not set a high standard for privacy protection; on the contrary, it legitimises social media platforms to collect and use personal data of individuals based on a fictional consent. This legal fiction has allowed social media platforms to track individuals unlimitedly, by collecting not only the information they choose to share voluntarily but also their actions, their movements, their routines, their companions and even their private messages.

In the meantime, personal data is being used by social media platforms to manipulate human will and to control the results of democratic processes. It is necessary to rethink regulations for an effective protection of privacy. Also, it is imperative to regulate social media platforms to limit their power over individuals and society.

[64] Solove, supra note 18, at 1881.

[65] Anita L Allen, 'Unpopular Privacy: The Case for Government Mandates' (2007) 32 Okla City U L Rev 87, 102.

## The Law Journal of the Association of Lawyers in Intergovernmental Finance and Development Organisations (ALIFDO) Ltd.

www.alifdo.com

The Intergovernmental Organisations In-house Counsel Journal is the law journal of the Association of Lawyers in Intergovernmental Finance and Development Organisations (ALIFDO) Ltd.. It is published electronically once every two years and is free of charge to the public.

The purpose of the journal is to provide a platform for ALIFDO members, academics and other practitioners, to identify and explore topics of interest to lawyers working for international organisations committed to finance or development, and to those who are interested in the work of these organisations.

Founded in 2017 by in-house lawyers working at the time at the European Bank for Reconstruction and Development, the World Bank and the Asian Infrastructure Investment Bank, ALIFDO now counts over 400 individual members working at 20 international organisations. ALIFDO is an individual membership-based organisation for lawyers working, in whatever capacity, for intergovernmental organisations committed to finance or development. For more information, please visit ALIFDO's website: www.alifdo.com.

An up-to-date listing of organisations where ALIFDO has individual members can be found at www.alifdo.com/membership

### Subscriptions and Future Issues

The IOICJ is published online on ALIFDO's website at www.alifdo.com/the-intergovernmental-organisations-in-house-counsel-journal
Print editions are currently not available.

To be added to the IOICJ's mailing list, please go to http://eepurl.com/gTQThT.

ALIFDO

ALIFDO