EU and AI: EU Identity and "Systemic Rivalry"

Robert Gould[1]
Carleton University

February 2021

Commentary written for the Jean Monnet Centre of Excellence, which is supported by a grant from the Erasmus+ Programme of the European Union. The Jean Monnet Centre of Excellence is housed at Carleton University in Ottawa, Canada, https://carleton.ca/ces.

For further discussions of digital issues relating to the EU, please see Danet et al. and Bendiek in the EU Policy Briefs section of the CES Research and Publications section.

With the support of the Erasmus+ Programme of the European Union

Background

[1] Robert Gould is a Canada-Europe Transatlantic Dialogue collaborator and Adjunct Research Professor in the Institute of European, Russian and Eurasian Studies at Carleton University.

Starting from my commentary "EU digital Autonomy, Sovereignty and Identity in the Time of COVID-19" (Gould 2020) and points made by my colleague in EURUS, J Paul Goode, in his recent article "Artificial Intelligence and the Future of Nationalism" (Goode 2020), this commentary will consider the stated desire of the European Union to promote digital R and D and an EU-based AI industry in order to serve the people of the EU and also mankind (see below) in a manner which is in conformity with EU values and principles. This development is to receive very significant funding from Brussels as part of the (admittedly reduced) post-COVID development fund. At the same time, such an effort will or would increase the presence and influence of a third force in the current world-wide digital duopoly of the United States and China.

In the 2020 commentary I expressed a degree of scepticism about the ability of the Union to fulfill its pledges and stated policy because of the strain placed on national and supranational budgets due to the negative impact of COVID-19 on economic activity. This means the consequent necessity of providing financial support to individuals and businesses because of losses suffered resulting from the confinement policies imposed for public-health reasons. This theme will not be investigated further in this commentary, but it will always be in the background, hence, on occasion, the hesitant nature of some of the conclusions. The commentary will, instead, examine implications arising from the urgent necessity proclaimed by the EU to extend and reinforce a Europe-based AI and digital industry.[2]

Goode concentrates his discussion on two foci: the nation state (including cultural homogenisation and inter/intra-national rivalries and nationalism) and, to a lesser extent, global corporations. In no way does this commentary call into question the validity of these foci and the accompanying argumentation. It wishes instead to take some of the arguments Goode makes and to extend them beyond the nation state to the level of the European Union as a whole, particularly in areas relating to AI and digital R and D.

Introduction

This commentary will draw attention to implications of the possible implementation of an EU-European AI industry arising from the assertion of EU identity, and in particular an increase in rivalries. This would result from the exercise of a soft or not-so-soft power partly by electronic means; this is made possible by market size, by the attractiveness (in some countries at least) of the assertion that privacy is a human right (see below), and by carefully-nurtured cooperation based on the previous two factors (Schwartz 2019). It is the expression of identity on a larger geographic scale than that of the individual nation; using the possibilities, both present and future, brought about by technological change it is the practical assertion of a distinct value-system. This is being undertaken by means of legislation from above (the Commission and the European Parliament) according to first principles of the Union as anchored in the foundational treaties. It might well be

[2] For further information on developments see, for example, Bendiek and Schallbruch 2019.

argued that in some measure this is occurring in response to forces being exercised by foreign-registered large international commercial entities physically operating, or providing services, in the EU. These global businesses incorporate, represent and exercise in whole or in part either Chinese or US value systems (see my previous commentary mentioned above and some comments below). The resistance to these forces is not due to popular pressures or practices, or to political parties' desire for electoral success at the nation-state level through the assertion of 'ancient' or 'traditional' values and 'sovereignty' such as are programmatically announced, for example, in the names of VOX España, Alternative für Deutschland and the United Kingdom Independence Party, or strongly implied in Front national / Rassemblement national in France. To repeat what is fundamental: it is the assertion of identity through the practical application from above of humane values not tied to any individual state, but rather tied to and characterising a particular bloc of states.

On the other hand, what is clear is that the EU is acting in a manner parallel to statements made by such nationalist-oriented parties as were just mentioned in that it is seeking to protect a conception of identity in the face of perceived threats coming from outside the Union and operating within the Union. It is not protecting individual countries and what is claimed to be a traditional or 'national' way of life. On the contrary, one might argue that with the strong emphasis on ethical applications and the protection of privacy, both fundamental to the EU's stance on web-based information processing, the EU is in fact emphasising a characteristic of group identity quite distinct from that existing in each of the rivals in the current duopoly of China and the US (see for example Lee 2019). In moving to intrude further in this duopoly the EU is inserting in a more forceful manner a different set of values on the international scene and thus is moving further into a position of rivalry. This commentary will explore this theme which is implicit, but very real, in relation to the US, and explicit, and increasingly real, in relation to China.

In my earlier commentary the EU's position on the present and future importance of AI is outlined from various published documents, and need not be repeated here. In the interim the awareness of the wide scope of possible AI applications has not been modified or restricted by other EU or civil-society publications. There is continuation of agreement that the impact will be far reaching in all areas of civil life and state operations. Nor is the end-point any clearer, only the repeated assertion that it presents significant military advantages, will modify the structure of the labour force, but will undoubtedly also improve human life while at the same time creating significant ethical and privacy concerns (for example McKinsey 2018, Taulli 2019, CIFAR 2020). This position deriving from an assessment of the present and unclear future scope of AI and its applications is the constant background to the commentary.

In the following discussion most of the examples of a different value system from that of the EU will refer to the United States. However, in the Introduction to its Communication *EU-China – A strategic outlook* (EU 2019a) the Commission makes a fundamental point, "…**there is a growing**

appreciation in Europe that the balance of challenges and opportunities presented by China has shifted" (p. 1, bold in the original). It stresses also the importance of maintaining Europe's social model over the long term (p. 2), and reiterates its desire to develop and deploy "cutting-edge, ethical and secure Artificial Intelligence" (p. 9). At the same time, the Communication states openly that China is a "systemic rival promoting alternative modes of government" (p. 1). This confrontation with China is so stark that the Commission warns "Neither the EU nor any of its member states can effectively achieve their aims without **full unity**", (p. 2, bold in the original). The fundamentals here are no different from the forces and dynamics with reference to the US, though not in terms of "alternative modes of government", rather, in terms of the (power) relationship between the individual and business.

The starting point for Goode's paper is his view that the new defining element of state sovereignty is the shift "from territorial control to the management and manipulation of population data" by electronic means. This commentary will take the notion two, or even three, steps further: EU 'sovereignty' (to continue using this term) is anchored not just in the management and manipulation of population data by the state or Union according to its vision of an ethical and human-centred society (see Gould 2020), but also in its influence on commercial and other entities. And this is not just at the national level, but also at the supranational and global levels. And given the very extensive world-wide dimension of the movement of goods and services into and out of the EU or the activities of non-EU businesses within the EU (think Amazon, for example) and the consequent gathering of personal and commercial information this entails, the implications of this are indeed global.

Through the existence, nature, acceptance and influence of the General Data Protection Regulation (EU 2016; see the following section **Data Eco System** for more information) the EU has established itself as both a benevolent and also globally influential force in the area of privacy protection in the digital sphere (Schwarz 2019; Bradford 2012 and 2020). The challenge will be to protect and maintain this influential expression of values forming part of EU identity during any future establishment and operation of a European AI industry. It is clear that in the EU and Europe there is no shortage of researchers in the forefront of developing digital data processing, and particularly AI and its implementation. However, and it is an important however, given the vast amounts of cash and other liquid assets which the very large American technology companies have available for purchases and takeovers (see Gould 2020), once a new and valuable EU-European AI or other digital product has been established and scaled up, will the product remain within the EU, under EU-based control, and reflecting EU values? This question of takeovers cannot be addressed here, but the recent comment in *The Economist* that "Capital is always relatively scarce in Europe compared with America" (Charlemagne 2021) points again to a real problem. Clearly, if it is not seriously taken into consideration at the level of the Commission, then the development efforts will have been for nothing.

The judgement on 16 July 2020 by the European Union Court of Justice in the Schrems case (C-311/18 Facebook Ireland and Schrems) declared the EU-US Privacy Shield invalid as it did not meet the requirements of GDPR. The civil society organisation *noyb.eu* European Centre for Digital Rights has more recently published information and correspondence with a wide range of US technology companies gathering and processing personal date of EU residents. The Centre's report *Opening Pandora's Box: How companies addressed our questions about their international data transfers after the CJEU's ruling in C-31/18 - Schrems II* (noyb.eu 2020a) makes clear the unwillingness of many US technology companies to follow the requirements of GDPR. In some cases it even reveals the companies' ignorance of their obligations (*noyb.eu* 2020b). Also, Section 14 of the (US) Executive Order 13768 of January 25th 2017 "Enhancing Public Safety in the Interior of the United States" (Federal Register 2017) (although contested) denies protection of personal data in the United States to any persons other than US citizens and residents once national security is invoked. Perhaps because of the sheer size and market power of Google Analytics and Facebook Connect, EU-domiciled companies are continuing to send data to the US, despite the judgement of the EUCJ (noyb.eu 2020c). Consequently, despite the apparently benevolent situation outlined by Schwartz above, it is clear that European data being in any way processed by servers under American control has in actual fact currently few or no privacy protections. This situation may well not be resolved to European satisfaction in the foreseeable future. This indicates that there is a situation threatening the effective existence of that part of EU identity expressed and made concrete in GDPR. At the same time, it indicates the real need for the development of an EU-based AI and digital R and D within the EU.

Deriving from Goode's discussion, the points to be considered next are the following: i) the data ecosystem; ii) the move away from nationalism, national practices and inter-nation rivalry; and iii) structural power hierarchies. These have been chosen as they demonstrate well the interplay of forces in the matters under discussion and the move towards bloc rivalry.

Data Ecosystem

The over-arching concept in this discussion is the data eco-system. For the purpose of this commentary the foundation of this is considered to be the General Data Protection Regulation (EU 2016). Approved on 14 April 2016 and implemented on 25 May 2018, broadly speaking, it regulates the processing and confidentiality of all data pertaining to individuals resident in the European Union, stating as first principle that "The protection of natural persons in relation to the processing of personal data is a fundamental right" (Preamble, Item 1), that "The processing of personal data should be designed to serve mankind" (Preamble, Item 4) and this is "regardless of whether the processing takes place in the union or not" (Art. 3, Paragraph 1). Explicitly, it is to apply also to personal data processed by administrative or legislative bodies of the Union itself (Preamble, Item 17).

I am emphasising here that with the entry into force of the GDPR in 2018 the European Union has already gone, or attempted to go, beyond the national and EU dimension to reach into a global dimension. No matter where in the world their human data processers, programmers, decision makers and their servers may be located, all companies and other entities communicating electronically with individuals or businesses within the EU and EEA and obtaining personal data from them, or providing services to individuals and entities located in the EU, are, in theory, bound by this regulation. Breaches are subject to very significant fines up to up to 20 million euros or 4% of a company´s world-wide revenue (whichever is greater) and even to criminal penalties. But, as was indicated in the previous section, compliance and enforcement are a different matter.

To cite just one concrete and representative example of the inevitable impact of this regulation if companies choose to adhere to it: in March 2018 BDO Canada, a member of the global accounting and business consulting network BDO International Limited, published a White Paper "How Canadian Companies can prepare for GDPR Compliance" (BDO 2018). It provides an overview of the three major areas of commercial digital activity where compliance is required. These are if the business is a) "offering goods or services to EU residents", or b) if it is "monitoring the behavior of EU residents within the EU, which may include tracking internet activity for behavioral advertising purposes", or c) if it is "conducting business with or in the EU, or marketing goods and services to EU residents". The White Paper then indicates in more detail the steps a business has to take in order to reach and maintain compliance and offers the services of BDO to aid businesses to place and maintain themselves in compliance with this piece of EU legislation.

Clearly, it follows that whatever practical consequences and commercial activities will arise within the Union and from the EU's promotion of a European AI industry and digital R and D, and no matter where they are or where they will provide services, such activities and consequences will be obliged to follow the GDPR or any subsequent EU legislation applicable in this area. And any non-EU AI business wishing to interchange personal data or submit data will have to certify compliance with the EU standards reflecting a conception of European identity. But as indicated in the previous section, there is a real problem of enforcing compliance in the face of reluctance and national regulation in the US.

This leads inevitably to the following:

The move away from nationalism, national practices and inter-nation rivalry.

In his consideration of AI activities at the national level, Goode includes the issues of the not unrelated concepts of "cultural bias" and "data colonialism", seeing in them possibilities for the creation or intensification of nationalism and international rivalries. Certainly, the GDPR contains a cultural bias, which, through the argument I have just laid out above, implies that any development of an EU-European AI industry will contain a cultural bias. It is asserting the superiority of EU values in the areas of privacy protection, transparency of use and control of use.

To some extent, one or the other of these may be or in the past may have been breached by certain practices and policies of member states and European businesses, but the legislation is insisting that these stop for the sake of equality and equity across the whole Union. Thus (with certain restrictions applying to national security, for example) this cultural bias expressed in EU legislation trumps national legislation, national practices and values and potentially impacts national identity, substituting Europe-wide notions of individuality and privacy for whatever values were previously held locally. It is conceivable that in the long run these administrative concepts will gradually filter down and affect individuals' thinking concerning privacy and thus this aspect of identity also.

As has been indicated, the GDPR applies also outside the Union where, certainly, it comes into conflict with national legislation and/or commercial practices, as indicated in my 2020 commentary and in the previous section of this one. To cite just one concrete example of the violation of European practices as defined in GDPR: in June 2020 the Spanish journalist Jordi Pérez Colomé published a report that his images and those of two other residents of the EU (in another EU member state) were stored and being made commercially available by Clearview AI (located in the US) without the knowledge or consent of himself or of the other EU residents concerned[3] (Pérez Colomé 2020). On the basis of that one reference one could reasonably conclude that there were far more than just these three cases of mis-use of images of EU residents and that this mis-use extended into all member states and an untold number of people. In fact, as was just made public in a long investigative article in the New York Times Magazine of 21 March 2021, the number of searchable images held by Clearview AI is currently put at three billion (this is not a typo: it is 'billion' with a b). The total number of EU residents whose images were captured from publicly-available sources and then offered for commercial purposes without their knowledge or consent – clearly contrary to GDPR – is quite possibly, and even probably, in the millions. This (mis-) use has been, and is currently being, defended in the United States under the First Amendment right (Hill 2021). The clash of EU legislation and US practice and jurisprudence could not be clearer.

Thus it is clear from this particular revelation and the obstacles outlined in the previous section that, in the case of EU-Europe at least, inter-national rivalry has been / is being flattened and replaced by inter-bloc rivalry, with the US (in the form of its government and American commercial enterprises) as a powerful well-established force *de facto* in opposition to the value of personal privacy and control incorporated as part of EU identity and legislation. Such an inter-bloc rivalry inevitably also applies to China, as noted above, now defined by the EU as a "systemic rival" (EU 2019a and see above).

This raises two questions, very real but both unanswerable at the moment: in this respect, what will happen in the United Kingdom now that it has left the EU and the transition period is over?

[3] Ironically, one of the persons named in the article is a specialist in data protection law.

Will it move away from a position reflecting the EU identity and towards the more commercially and national security-oriented position of the United States? It appears that the Christmas-Eve Agreement is silent on this matter (as on so many others). Will it, now that it is alone, be capable of regulating companies thousands of miles away in California (*The Economist* 2021)? And what will happen with the numerous other countries which have created their own personal-data protection legislation following the model of the GDPR (see the section Structural Power Hierarchies below)? Would they, could they, in the future move to a position whereby they use EU-based AI and form a critical mass, thus placing a future EU AI industry in a stronger position in the face of the US or China? Rivalry will not disappear, and many of the concerns raised by Goode will remain, but it is conceivable that what such developments will reinforce will be above all inter-bloc rivalry.

Data Colonialism

On the question of "data colonialism" raised by Goode and others, while the EU is certainly insisting on a degree of extra-territoriality for its legislation (GDPR Article 3) and implicitly views it as superior to other practices in the area of data protection (or non-protection), it cannot impose it and does not claim to impose it on entities in other jurisdictions which are not processing the data of EU residents. But it does, as Goode says, "diminish[...] the boundaries of national identities" to the extent that it seeks to diminish distinctions between what are considered appropriate and acceptable social practices in one or the other EU country, and between EU practices and non-EU practices. And appropriate and acceptable social practices, which include the interactions between corporate entities and natural persons, are certainly part of a national identity. One can therefore say with Goode, although he is thinking in terms only of individual nations, that the GDPR and its present and future impact on AI "challenge existing social, political and economic structures at the same time that [they] replicate[…], incentivize[…] and secure[…] [the EU] as a social form and source of political [and one must add: social] legitimacy in everyday life". The extent of "this (successful) challenge to existing social, political and economic structures" can be glimpsed by reference to Bradford (2012). Written before the introduction of the GDPR and thus referring only to the less stringent regulation of privacy under the previous EU data regime (Directive 95/45/EC), it outlines how global business, and particularly US business, had been pushed by market pressures and insistence on conformity with EU regulations to accept, or to appear to accept, EU standards. This occurred frequently unwillingly as the EU standards conflicted with the corporate values deriving from the purely American social and economic identity they previously possessed because of their origin and location in the US. American (corporate) identity was challenged and potentially will be challenged more seriously to the extent that the EU can be successful in promoting a Europe-based AI industry operating on a world-wide scale and potentially even processing the data of US residents. The continuing opposition by US-based global businesses to accept EU jurisdiction as it impacts their corporate culture, practices and identity is evident from court cases and investigation (see above and Gould 2020). A stronger European AI industry could conceivably reduce such conflicts by reducing the amount of EU-

originating personal data being exported for processing. Conversely, it might lead to heightened tensions, recriminations and retribution resulting from its increased presence, challenge and rivalry in markets where hitherto it had been absent.

Similarly, while at least some non-EU businesses will continue to analyse data on EU residents within (one hopes) the constraints of EU law and then implement the results, hopefully also in a lawful manner, a strengthened European AI industry would certainly reinforce any unwillingness to export population data for commercial purposes wholesale and could even ensure it is totally unnecessary. This reduces, though does not eliminate, the possibility of indirect foreign control or more direct influence through, for example, a deep knowledge of spending habits which can arise through prolonged and intense use of foreign payment apps – hence the warning issued by the German Office for the Protection of the Constitution about the use of Chinese payment apps. This warning was made in conjunction with a further one concerning Chinese acquisitions of German "businesses in key technological areas" (see Gould 2020). These are country-specific warnings reflecting the statement of Action 10 of the Communication *EU-China – A strategic Outlook*: "To detect and raise awareness of security risks posed by foreign investment in critical assets, technologies and infrastructure, Member States should ensure the swift, full and effective implementation of the Regulation on screening of foreign direct investment" (EU 2019a).

The need for European-developed and European-controlled strategic digital enterprises emerges very clearly from this. European-developed AI does not serve European interests if it is not under European control. With its mandate to protect Germany, the (German) Office for the Protection of the Constitution is phrasing its warnings about international rivalries in purely national terms (the pattern of Goode's discussion), but for the EU the concerns are broader. Any type of what Goode terms the "outsourcing" (broadly understood) of European data has to be seen in EU rather than national terms.

The above considerations raise the issue of what Goode calls structural power hierarchies.

Structural Power Hierarchies

Goode views these in terms of "…average national lifestyles along with the biases and structural power hierarchies that code and sustain them", that is, aspects of national identity. As initially indicated, this commentary is explicitly taking this idea further. Within the European context a well-developed EU-European AI industry following GDPR and other privacy legislation such as the 2019 European Cybersecurity Act (EU 2019b) would certainly further flatten differences in online politically-mandated social or commercial practices between, among and within nations and member states. Beyond purely digital interaction this might conceivably spill over into the area of face-to-face and other personal interactions: for example, what information can a customer service representative ask of a potential or actual client that then would be recorded on a data base and included in later analysis? The same features / considerations would operate if a European AI industry is attractive in the at least 120 countries which have passed GDPR-influenced data

protection legislation and the thirty more that as of 2017 had bills to that effect (Schwartz 2019 quoting Greenleaf 2017. See also Bradford 2020: 152f for more details) to the extent that their businesses or other entities contract processing to European enterprises. Alternatively, given that their data protection legislation is indeed very close to GDPR and continues to follow its example, then, even without moving the data processing to Europe, the influences just described apply and conceivably impact society. Consequently, what is imaginable is the development beyond the borders of the EU itself of an EU-oriented bloc of nations aligning their digital identities and thus parts of their legal and social identities with those of the Union.

It can be argued also that, as indicated above, the unwillingness of established American digital businesses to adhere to or even to take seriously EU data privacy concerns is an example of a structural power hierarchy deliberately created by the American practice of enabling as many states and companies as possible to use US products and services (Schulze and Voelsen 2020). Asked the question in a recent interview "Is Europe more or less a tech colony of the Americans", Kai-Fu Lee, founder of Google China and now chairman of Sinovation Ventures, answered, "Yes it is […]. As you say, Europe is pretty much an American Colony". This suggests that in the form of its digital businesses the American quasi-colonial power considers itself in such a position of strength that it can do largely as it pleases and impose its will and data culture, even though, as Lee admits, "some differentiation is appearing" in Europe in the form of GDPR (Lee 2019).

What is happening here is, in Goode's words, "competition between global corporations and states" (where "states" is to be understood in this particular context as referring to the EU) concerning "standards of civilizational belonging": each wishes to impose its respective set of values. The brief reference above to the German warning about the use of Chinese payment apps and the shared German and EU warnings concerning corporate acquisitions of strategically important businesses indicate this other participant in the would-be quasi-colonial and / or structural power struggle to impose a hierarchy of values: the attempt by China to place itself in a position of greater influence in at least some parts of the world, and even to challenge what Lee views as the hegemon in the "American [data] colony" of Europe. To revert to the statement in the Introduction, the problematic nature of the Commission's assertion of European values and identity vis-a-vis China is evident in its definition of the EU's relationship with that country as simultaneously "…an economic competitor in the pursuit of technological leadership and a systemic rival promoting alternative models of governance" (EU 2019a). This is the crux: the clash of hoped-to-be technology and real-existing systemic rivalry in the promotion of models of governance, where 'models of governance' implies views of the nature of the individual's rights and the relationship between individual and the state, and also between individual and business. For each party in this confrontation defined by the Commission (EU and China) and for each party in the confrontation outlined earlier (EU and US), it is a clash of group identity and (implicitly) also of personal identity in the form of the relationship between the individual and the state / business.

But leaving side aside the veracity or not of an easily-asserted and attention-grabbing term "American colony" used in an interview, it is quite clear that the desire to establish an effective EU-based AI industry in such a way that other jurisdictions would have to conform to its values and practices means that the so-called "American colony" is biting back. It is following past practice, as Bradford (2020) lays out more fully, of exporting its "standards of civilization" (Bradford 2012) through structural power in what some who wish to denigrate the European Union, its distinct identity and its growing role in the world have called a "neo-colonial" or "imperialist" manner (see opinions quoted in Bradford 2012).

Similarly, one can argue that, with respect to data protection, the EU-China Comprehensive Agreement on Investment (finally agreed in principle on 30 December 2020) also contains an attempt to assert "its standards of civilization" and thus a part of the EU's identity and values in the face of its "systemic rival". With this step it aims to check some of the perceived (mal)practices of the latter. Article 1, Paragraph 2 of the agreement in principle explicitly refers to "privacy and data protection" (EU 2021). The press release concerning the conclusion of the agreement mentions in first place "rules against the forced transfer of technologies" and later amplifies this initial statement with a section devoted to the topic, including in it also "protection of confidential business information collected by administrative bodies (for instance in the process of certification of a good or a service) from unauthorised disclosure" going beyond existing WTO rules (EU Commission Press Release 2020). This desideratum is in parallel with the protection of data concerning natural persons outlined throughout this commentary. The EU is insisting on data protection in the face of both the state and business, and also on behalf of business.

Conclusion

Undoubtedly, both the United States and China are nation states each with its own set of economic and cultural values as part of an identity projected on to the global scene *inter al.* in the form of economic and soft-power self-assertion. In the light of the foregoing commentary one can perceive a struggle to impose an EU-based AI presence following EU rules which will be a "national brand" with "the cultural authority to codify the social, economic and cultural practices which codify …practices that define a nation" (Goode 2020), and would effectively impose them elsewhere. In this connection and for this commentary 'Nation' is once more to be interpreted as referring to the EU as a whole. At stake is the reinforcement and enforcement of an important aspect of the present and future global presence of the European Union, a further effective expression of its distinct identity and cultural values. Although not a state, it is following imperatives relevant for states in order to protect, define and realise its interests and identity. And in wishing to do this more strongly on a global scale it inevitably, and now overtly, moves further into a situation of rivalry with what is now acknowledged to be a "systemic rival promoting alternative modes of government".

Key Words: European Union, Artificial Intelligence, GDPR, China, USA, Rivalry

References

BDO. 2018. *How Canadian Companies can prepare for GDPO Compliance.* White Paper. Available at https://www.bdo.ca/en-ca/landing-pages/gdpr-compliance/ .

Bendiek, Annegret and Martin Schallbruch. 2019. "Europe's third Way in Cyberspace: What part does the new EU Cybersecurity Act play?". *SWP Comment* 52, Berlin. Stiftung Wissenschaft und Politik:1-8.

Bradford, Anu. 2012. "The Brussels Effect". *Northwestern University Law Review* vol 107, no. 1: 1-66.

Bradford, Anu. 2020. *How the European Union Rules the World*, Oxford, OUP, online version DOI: 10.1093/oso/9780190088583.001.0001.

Charlemagne. 2021. "Cyberpunked". *The Economist.* January 16th-27th, vol. 438, number 9228: 42.

CIFAR 2020. *AICan 2020: CIFAR Pan-Canadian AI-Strategy: Impact Report*, Canadian Institute for Advanced Research, Toronto 2020.

The Economist. 2021. "Chlorinated Facebook". January 9th-15th, vol. 438, number 9227: 48.

EU. 2016. *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 (General Data Protection Regulation).* Brussels. available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN .

EU. 2019a. *EU-China – A strategic outlook*. Brussels, EU Commission.

EU. 2019b. REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA. Brussels. *Official Journal of the European Union* L 151/15. June 7.

EU.2021. EU-China Investment Agreement. Available at https://trade.ec.europa.eu/doclib/docs/2021/january/tradoc_159342.pdf .

EU Commission Press Release. 2020. Key Elements of the EU-China Comprehensive Agreement on Investment. 30 December 2020. Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2542 .

Federal Register. 2017. / Executive Order 13768 "Enhancing Public Safety in the Interior of the United States Presidential Documents. Vol. 82, No. 18. Monday, January 30: 8799.

Goode, J Paul. 2020. "Artificial Intelligence and the Future of Nationalism" *Nations and Nationalism*: 1-14

Gould, Robert. 2020. "EU Digital Autonomy, Sovereignty and Identity in the Time of COVID-19". Commentary available at https://carleton.ca/ces/wp-content/uploads/Robert-Gould-EU-Digital-Autonomy-Sovereignty-and-Identity-in-the-Time-of-COVID-19-final.pdf .

Hill, Kashmir. 2021. "Your Face is not your own", New York Times Magazine: 21 March: 32-49. Available on the web at https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html (viewed 21 March 2021).

Lee, Kai-Fu. 2019. "The Great AI Duopoly", *New Perspectives Quarterly* 36 (1): 27-32.

McKinsey Global Institute (2018), *Notes from the AI Frontier: Applying AI for Social Good.* Discussion paper.

CIFAR 2020: Pan-Canadian AI-Strategy: Impact Report Canadian Institute for Advanced Research. Toronto 2020.

Schulze, Matthias and Daniel Voelsen. 2020. "Digital Spheres of Influence" in *Strategic Rivalries between the United States and China: Causes, Trajectories and Implications for Europe.* Edited by Barbara Lippert and Volker Perthes), *SWP Research Paper* 4, April 2020. Berlin. Stiftung Wissenschaft und Politik.

Noyb.eu. 2020a. *Noyb.eu*European Centre for Digital Rights. "Opening Pandora's Box: Companies can't say how they comply with CJEU ruling" available at https://noyb.eu/en/opening-pandoras-box-companies-cant-say-how-they-comply-cjeu-ruling (viewed 13 January 2021).

Noyb.eu. 2020b. *Noyb.eu*European Centre for Digital Rights "Opening Pandora's Box: How companies addressed our questions about their international data transfers after the CJEU's ruling in C-31/18 - Schrems II" Available at https://noyb.eu/files/web/Replies_from_controllers_on_EU-US_transfers.pdf?mtc=j , (viewed 13 January 2021).

N*oyb.de*. 2020c. "Update on *noyb's* complaints on EU-US Data Transfers: Only one country shines". Available at https://noyb.eu/en/update-noybs-101-complaints-eu-us-data-transfers (viewed 22 January 2021).

Pérez Colomé , Jordi 2020. "La empresa que almacena fotos tuyas en Internet para identificarte". El País, 16 June. Available online https://elpais.com/tecnologia/2020-06-16/la-empresa-que-almacena-fotos-tuyas-en-internet-para-identificarte.html .

Schwarz, Paul M. 2019. "Global Data Privacy: the EU Way". *New York University Law Review* 94: 771-818

Taulli, Tom. 2019. *Artificial Intelligence Basics.* Available online https://doi.org/10.1007/978-1-4842-5028-0_9 , Chapter 9, no pagination. Berkeley. Apress.

.