THE CAPCO INSTITUTE

JOURNAL

OF FINANCIAL TRANSFORMATION

CYBER

Europe's push for digital sovereignty: Threats, E.U. policy solutions, and impact on the financial sector

LOKKE MOEREL

CLOUD

#55 MAY 2022

a **wipro** company

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

CLOUD

CRYPTO

CYBER

DEAR READER,

Welcome to edition 55 of the Capco Institute Journal of Financial Transformation. Our central theme is cloud computing, which has transformed from an efficiency initiative for our clients, to an indispensable growth driver for financial services.

The pandemic has changed consumer expectations, with consumers now demanding 24/7 access to their financial resources from anywhere, as well as hyper-personalized products that reflect their lifestyle choices.

In this edition of the Journal, we explore the power of cloud and its potential applications through the lens of a joint Capco and Wipro global study, and take a deeper look at the financial services data collected in Wipro FullStride Cloud Services' 2021 Global Survey. The survey was focused on perceptions of cloud and its importance to business strategy from over 1,300 C-level executives and key decision-makers across 11 industries.

The study indicates that cloud is becoming ever more intelligent, hyperconnected, and pervasive, and enables companies to offer their end users the personalized, user-centric experience that they have come to expect. It's clear that only the financial services firms that can successfully leverage cloud, will thrive.

In addition, this edition of the Journal examines important topics around digital assets and decentralized finance, including central bank digital currencies, and bitcoin's impact on the environment, and cybersecurity and resilience.

As ever, you can expect the highest calibre of research and practical guidance from our distinguished contributors, and I trust that this will prove useful in informing your own thinking and decision-making.

Thank you to all our contributors and thank you for reading. I look forward to sharing future editions of the Journal with you.

Lance Levy, **Capco CEO**

EUROPE'S PUSH FOR DIGITAL SOVEREIGNTY: THREATS, E.U. POLICY SOLUTIONS, AND IMPACT ON THE FINANCIAL SECTOR

LOKKE MOEREL | Professor of Global ICT Law, Tilburg University*

ABSTRACT

The European Union (E.U.) feels the threat of what is coined digital colonialism of the U.S. and China,[1] where the E.U. member states are increasingly dependent on digital infrastructures that are in the hands of a handful of dominant foreign market players. The digital identity of most European citizens depends on foreign email addresses, and a staggering 92 percent of European data reside in the clouds of U.S. technology companies, of which 80 percent are with five suppliers only.[2] Besides supply chain dependencies, these companies operate proprietary ecosystems, which offer limited interoperability and portability of data and applications, resulting in E.U. data being locked-in and having limited value for E.U. innovation.[3] Restoring Europe's "digital sovereignty" is now a core ambition of the European Commission (E.C.); however, achieving it at a time when digital technologies have become the battleground for the race for global leadership between the U.S. and China (aka the tech cold war) will not be easy. Both the U.S. and China regularly draw the national security card to justify stricter export controls of critical technology and bringing manufacturing back to their countries. Recent U.S. executive orders ensure that almost any ICT-related activity in the U.S. connected to China is now subject to regulatory review by the U.S. government. Not surprisingly, China is retaliating.

With the E.U. policy measures, the E.C. is aiming to pave a third way, in order to avoid falling into the trap of tech protectionism. Flagship initiatives discussed are the so-called European Data Spaces (bringing together E.U. data of specific industry sectors in order to unlock their value for E.U. innovation) and the GAIA-X project (achieving interoperability between cloud offerings to achieve the required scalability for AI-related innovations, without setting up European hyperscalers). All initiatives will also have a fundamental impact on the business models of the financial sector. This article discusses the threats to E.U. digital sovereignty in order to help the reader better understand the E.U. policy proposals and their disruptive impacts, which – as with any regulation – brings new requirements, but also opportunities for innovation.

* Lokke Moerel is also a member of the Dutch Cyber Security Council. This article is based on an earlier article: Timmers, P., and L. Moerel, 2020, "Reflections on digital sovereignty," E.U. Cyber Direct, January 15, https://bit.ly/3s7sz2K, originally written in assignment of the University of Utrecht 2020 Annual Constitutional Law Conference: Constitutional law in the data society.

[1] Kwet, M., "Digital colonialism: US empire and the new imperialism in the global south," Race & Class 60:4, 3-26.

[2] Amiot, E., I. Palencia, A. Baena, and C. de Pommerol, 2020, "European digital sovereignty: syncing values and value," Oliver Wyman, https://owy.mn/3L0pGf7.

[3] Digital Services Act package, Inception Impact Assessment, https://bit.ly/34TSe6u.

1. INTRODUCTION

Europe is one of the most digitalized societies and this has been accelerated by the COVID-19 pandemic.[4] Within no time, people worked from home and children were schooled online. It was amazing to see how quickly we were up and running again. However, as we become increasingly digitized, the vulnerabilities that come with it also increase. 2020 saw a 70 percent increase in internet-related crime, including COVID-19 scams,[5] a 150 percent increase in ransomware attacks exploiting work-from-home technologies,[6] hostile states trying to steal our COVID-19 research,[7] China and Russia pushing "fake news" to undermine our governments' COVID-19 responses,[8] and difficult-to-combat online conspiracy theories of anti-5G movements, stimulated by Russian infiltration.[9]

By now, the realization has set in that Europe's digital dependencies are so great that the digital sovereignty[10] of the E.U. and its member states is under pressure. The fears are justified, E.U. sovereignty (as the sovereignty of any state around the world for that matter) is under pressure due to a toxic combination of disruptive digital transformation (with winner takes all suppliers), exponential growth of cyberattacks (in which smaller countries and non-state actors now also enter the global battlefield), and rising geopolitical tensions, leading to a sovereignty gap.[11] Where at first digital sovereignty was discussed in the context of cybersecurity, military, and defense, the discussion now extends to concerns about the economy and society at large. The ultimate challenge is how Europe and its member states can retain control over their **economies** (control over essential economic ecosystems) and their **democracies** and **the rule of law** (trust in their legal system and quality of democratic decision-making) in the digital world.[12] Due to the multifaceted nature of the causes of the pressure on our digital sovereignty and rapid geopolitical developments, there is no one-size-fits-all solution. To be able to understand the series of E.U. policy initiatives to restore Europe's digital sovereignty, it is important to understand why Europe's ability to take decisions autonomously is under threat.

> *"We must have mastery and ownership of key technologies in Europe. These include quantum computing, artificial intelligence, blockchain, and critical chip technologies. (...) We need infrastructure fit for the future, with common standards, gigabit networks, and secure clouds of both current and next generations."*
>
> **Ursula von der Leyen** – *inaugural speech as president-elect European Commission (2019)*

Sovereignty is a political concept for which there is no generally accepted definition. Sovereignty is generally associated with territoriality, jurisdiction, a population, and authority with both internal and external recognition (legitimacy).

Internal legitimacy refers to the effectiveness of the state when executing governmental tasks (e.g., being in control of the electoral process and the criminal justice chain) and also the recognition by citizens of the government (having confidence in the rule of law).

External legitimacy concerns the recognition by foreign states and the autonomy of action toward such foreign states.

Strategic autonomy: if sovereignty is the goal, strategic autonomy is the means, i.e., the capabilities to decide on key aspects of the long-term future in the economy, society, and democracy.

[4] The European data economy continues to grow rapidly – from €301 bln (2.4 percent of GDP) in 2018 to an estimated €829 bln (5.8 percent of GDP) by 2025. IDC, 2020, "The European data market monitoring tool key facts and figures, first policy conclusions, data landscape and quantified stories," final study report, https://bit.ly/3BDBRGQ.
[5] FBI National Press Office, 2021, "FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics," Federal Bureau of Investigation, March 17, https://bit.ly/3p62T4V.
[6] https://bit.ly/3p29NrG.
[7] Grierson, J., and H. Devlin, 2020, "Hostile states trying to steal coronavirus research, says UK agency," The Guardian, May 3, https://bit.ly/3s8mLpN.
[8] Scott, M., 2020, "Russia and China push 'fake news' aimed at weakening Europe: report," Politico, April 1, https://politi.co/3LOate7.
[9] Lynas, M., 2020, "Anti-vaxxers and Russia behind viral 5G COVID conspiracy theory," Alliance for Science, April 8, https://bit.ly/3BGv0wj.
[10] For definitions see: Timmers, P., 2019, "Strategic autonomy and cybersecurity," E.U. Cyber Direct, May 10, https://bit.ly/3v67gAu.
[11] Timmers, P., 2019, "Challenged by 'digital sovereignty,'" Journal of Internet Law 23:6, 1, 18.
[12] See for in-depth discussion see Timmers, P., and L. Moerel, 2020, "Reflections on digital sovereignty," E.U. Cyber Direct, January 15, https://bit.ly/3s7sz2K.

2. WHAT ARE THE THREATS?

2.1 Disruptive digital transformation

Friends and foes agree that our society is undergoing a digital revolution (in official terms: the fourth industrial revolution) that will lead to a transformation of our society as we know it.[13] In addition to all economic and social progress and prosperity, every technological revolution also brings with it disruption and friction. The first law of technology is that it is not good, not bad, but also not neutral.[14] The new digital technologies (and, in particular, artificial intelligence (AI) and quantum computing) are in and of themselves already disrupting societies and create new vulnerabilities. Weakening control over innovation and knowledge can jeopardize sovereignty. For example, AI and encryption will play an increasingly crucial role in cyber resilience.[15] If there is not enough innovation, there will be new dependencies.

Current E.U. research investments in quantum computing and AI are dwarfed by the billions invested by the Chinese and U.S. governments,[16] combined with the investments from large U.S. and Chinese tech companies, such as Google[17] and Tencent.[18] Where foreign companies are at the forefront of (further) development and implementation of new technologies, such as AI and quantum computing, but also satellite and 5G networks, potentially new dependencies arise. These dependencies go beyond the specific technological applications themselves. For example, to be able to make large-scale use of data analysis by means of AI, enormous computing power is required. It is expected that the cloud infrastructure required for this will become the foundation for the European innovation and knowledge infrastructure. Maintaining control over this is an essential part of the E.U.'s digital sovereignty.[19]

EXAMPLE: AI AND CRYPTOGRAPHIC TECHNOLOGIES

With AI, bad actors can detect and exploit vulnerabilities automatically and on a large scale. However, AI is also expected to make it possible to automatically detect and restore vulnerabilities in software. We will, therefore, have to innovate to be able to keep ahead of bad actors.

Without proper encryption, we will not be able to protect the valuable and sensitive information of our governments, companies, and citizens. Current encryption will not hold against the computing power of future quantum computers. We will, therefore, have to innovate now to protect our critical information in the future. This is not only relevant for future information, but also for current information. Do not forget that currently hostile states systematically intercept and preserve encrypted communications in anticipation that these may be decrypted at a later stage and analyzed by deploying AI. We, therefore, have to invest in post-quantum encryption now in order to be able to protect strategic information that requires long-term protection.

2.2 Increasing cybersecurity threats

An important dimension of digital sovereignty is the cyber resilience of our critical sectors, processes, and data. The ever-increasing cybersecurity threats – in which smaller countries and non-state actors are now also entering the global battlefield[20] – undermine our digital sovereignty. These concern the entire spectrum of direct threats to our vital infrastructure (sabotage), systematic theft by foreign states of intellectual property from our knowledge-intensive industries (economic espionage), digital extortion (ransomware attacks), targeted misinformation (fake news), and systematic infiltration of social media to influence elections and democratic processes.

[13] For an accessible book, see Brynjolfsson, E., and A. McAfee, 2014, Second machine age: work, progress, and prosperity in a time of brilliant new technologies, W.W. Norton & Company, which gives a good overview of the friction and disruption that arose from the industrial revolution and how society ultimately responded and regulated negative excesses and a description of the friction and disruption caused by the digital revolution. A less accessible, but very instructive, book, on the risks of digitization and big tech for society is Zuboff, S., 2019, The age of surveillance capitalism, Public Affairs, [hereinafter: Zuboff (2019)].

[14] Kranzberg, M., 1986, "Technology and history: 'Kranzberg's laws'," Technology and Culture 27:3, 544-560.

[15] Van Boheemen, P., L. Kool, and J. Hamer, 2019, "Cyber resilience with new technology – opportunity and need for digital innovation," Rathenau Instituut, July 20, https://bit.ly/3LN7YsB. See also the Dutch Cyber Security Council Recommendation, 2020, "Towards structural deployment of innovative applications of new technologies for cyber resilience in the Netherlands," CSR Opinion 2020, no. 5, p. 3.

[16] See for an overview of U.S. and Chinese research investments, Smith-Goodson, P., 2019, "Quantum USA vs. quantum China: the world's most important technology race," Forbes, October 10, https://bit.ly/3sWJowv.

[17] In October 2019, Google claimed to have reached quantum supremacy with its Google quantum computer called Sycamore (https://go.nature.com/3JlJ9vL). On December 3, 2020, Chinese quantum computing researchers also claimed quantum supremacy (https://bit.ly/3vckY4W).

[18] Keen not to fall behind major U.S. tech firms in quantum computing, the Chinese company Tencent announced that it plans to invest U.S.$70 bln in infrastructure and quantum computing (https://bit.ly/3s7RkMc).

[19] Timmers, P., 2020, "There will be no global 6G unless we resolve sovereignty concerns in 5G governance," Nature Electronics 3, 10-12. See also the German "Industrial strategy 2030. Guidelines for a German and European industrial policy," (https://bit.ly/3t1c7Am) in which it is recognized that insufficient grip on new technologies poses a direct risk to the preservation of the technological sovereignty of the German economy.

[20] Sanger, D. A., 2018, The perfect weapon: war, sabotage, and fear in the cyber age, Scribe U.K.; Kello, L., 2017, The virtual weapon and international order, Yale University Press; Corien Prins also points out that the new digital weaponry is changing the (geopolitical) order: "The balance of power is shifting, now that smaller countries can also enter the global battlefield. Without having to engage in a large-scale military confrontation or actually enter the territory of another state. In short, it is relatively easy to develop great clout," https://bit.ly/3JOl8Td.

As far as cyber threats are concerned, digital sovereignty cannot be separated from the three basic principles of information security, also known as the CIA of cyber security: confidentiality, integrity, and availability. In these three domains, autonomy must be safeguarded, not only at the level of a specific system in a specific sector (such as an ICT system in the criminal justice chain), but also in the larger framework of the economy, society, and democracy.

For example, through a specific government ICT system, sovereignty can be undermined – think of stealing information from government officials for espionage purposes[21] (confidentiality) and cyberattacks on so-called industrial automation and control systems (IACS) in our critical infrastructure (availability). These systems are the specific targets of hostile states in order to make sabotage possible in the future as a means of pressure to achieve geopolitical objectives.[22] In these cases, we can translate digital sovereignty into direct requirements for ICT systems. These include requirements for security, threat detection, continuity (backup, disaster recovery), vendor lock-in (preventing dependence on a specific supplier), and access to data by foreign powers (encryption requirements). As indicated above, digital sovereignty, however, must also be translated into the broader state interest of economy, society, and democracy. Some examples to illustrate are listed below.

2.2.1 EXAMPLE: CONTROL OVER ESSENTIAL ECONOMIC ECOSYSTEMS

- **Economic espionage:** the systemic theft by hostile states of intellectual property and know-how of our high tech companies and universities undermines Europe's future earning capacity.
- **Cloud infrastructure:** we are becoming increasingly dependent on the digital infrastructures owned by a number of major foreign market players, which offer limited portability and interoperability of data and applications. For innovation with AI, you need large quantities of harmonized data and a lot of computing power to process these data. Individual companies do not have sufficient data to innovate and, therefore, the data of companies in a specific industry sector will have to be combined. This is currently difficult as the data of companies is stored in silos in the clouds of foreign tech providers. As a result whereof, these have limited availability for European innovation. Access to harmonized data and cloud-infrastructure will become the foundation for the European innovation and knowledge infrastructure. Maintaining control over this is an essential part of digital sovereignty.
- **Digital communications networks:** we are increasingly dependent on digital communications for the wellbeing of citizens and a strong economy. Think of video meetings and smart homes, but also new security-critical services such as smart energy grids, intelligent mobility systems, and remotely controlled care robots. The development and management of the underlying technical systems and networks (such as routers, switches, and DNS servers) are increasingly dominated by foreign parties. As a result, organizations and individuals have only a limited understanding of their dependencies on these parties and their systems, let alone control over them. This restricts our ability to decide autonomously and to act on how we set up our digital infrastructure and to which parties we want to entrust the transportation of our data.

IACS are the systems (hard- and software) that control our locks and bridges and ensure that energy and gas are distributed, drinking water is cleaned, and nuclear material is processed. IACS allow organizations to control their industrial processes locally or at remote locations and to monitor and process real-time data.

Vendor lock-in is caused by the fact that a supplier uses its own proprietary standards, which means that software and applications only work on its own platform, making a switch from one customer to another supplier costly or even impossible.

Portability is the ability of applications and data to be transferred – with reasonable effort – from one IT environment to another (the process of transfer, we call migration).

Interoperability is the ability of IT systems to work together with other IT systems, allowing data to be exchanged, and to use the data that has been exchanged.

[21] See, for an example: Bloomberg Law, 2020, "Chinese hackers targeted European officials in phishing campaign," September 2, https://bit.ly/3h3GxfN.
[22] For enemy cyberattacks on IACS in critical infrastructures, see: Gartner, 2019, "A report for the Dutch Ministry of Justice and Security, Cyber Security Research for Industrial Automation and Control Systems," August 21, https://bit.ly/3JKplbr; and the advice of the Dutch Cyber Security Council: "Advice on the digital security of Industrial Automation & Control Systems (IACS) in the critical infrastructure of the Netherlands," April 24, 2020 (CSC Advice on Cyber Security IACS), https://bit.ly/3BHIDeE.

2.2.2 EXAMPLE: CONTROL OVER DEMOCRATIC PROCESSES AND RULE OF LAW

- **Manipulation of election processes:** when our governments are not in control of important democratic processes like elections, it mainly affects the internal legitimacy of the state (the trust of citizens in the state). Where a state is not in control of the election process, because it has been infiltrated and manipulated by foreign powers, its external legitimacy may also be compromised. For example, during the pandemic, both China and Russia blatantly pushed "fake news" to undermine our governments' COVID-19 responses. This undermined not only the internal legitimacy of our governments, but also their external legitimacy. Whereas before COVID-19 China and Russia at least tried to hide their involvement in cyberattacks, they are now doing so blatantly. It shows Europe's weakness; these states do not fear that retaliations will be forthcoming, undermining the E.U.'s external legitimacy. Not President Biden – after the SolarWinds and Colonial Pipeline incidents, Biden made cyberattacks firmly part of the political discussions between states and warned Russia and China that continued cyberattacks could lead to a "real shooting war."[23]
- **Infiltration of a vital government process:** can also undermine trust in the rule of law. Illustrative is an incident in Germany. In January 2020, Der Spiegel reported that the Berlin High Court (responsible for terrorism cases) had been systematically infiltrated by a Russian hacker group probably sponsored by the Russian government, identified as APT 28 (Advanced Persistent Threat). This hacker group had previously been held responsible for the infiltration of the German Bundestag. The attack focused on data exfiltration, accessing the entire database with identities of suspects, victims, witnesses, and undercover agents, and informants.[24] These types of infiltration both undermine a governments' internal and external legitimacy.

2.3 Increasing geopolitical tensions

Europe's sovereignty is affected by the increasing trade and ideological tensions between the U.S. and China. The new digital technologies have become the battleground for the race for global leadership between the two countries (aka the tech cold war).[25] The battle is mainly about leadership in the fields of 5G/6G, quantum computing, computer chip technology, and AI. Both the U.S. and China have chosen the route of tech protectionism, regularly drawing the national security card to justify addressing critical supply chain issues (exposed by the pandemic) by bringing manufacturing back to their countries,[26] imposing stricter export controls of critical technology, and stepping up controls of foreign direct investments (FDI).[27]

Other examples of geopolitically motivated measures are President Trump's ban on Huawei as a supplier of U.S. telecommunications infrastructure, and the restriction on Huawei to purchase computer chips produced with U.S. technology outside the U.S.[28] Rather than specific restrictions on Huawei, President Biden issued a presidential Executive Order (amending President's Trump earlier ban), ensuring that almost any ICT-related activity in the U.S. is subject to prior regulatory scrutiny for Chinese involvement by the U.S. government.[29] Not surprisingly, China is retaliating.[30]

These examples show that the E.U. and its member states are limited in their sovereignty by geopolitically motivated measures taken by the U.S. and China. The E.U. increasingly finds itself the piggy-in-the-middle in a bipolar world, which hampers the E.U.'s policy options. This plays a role throughout Europe in, for example, the choice of suppliers for 5G equipment, for which Huawei was initially an important potential candidate. As a result, 5G, a critical digital infrastructure, is likely to become more expensive as the multivendor choice decreases. Over time, restrictions will likely extend to other equipment, such as Huawei servers that support cloud services, the presence of Chinese suppliers in the Internet of Things (IoT), cameras, airport scanners, and other surveillance equipment, and drones of Chinese origin.

[23] Manson, K., 2021, "Biden warns cyber attacks could lead to a 'real shooting war,'" Financial Times, July 28, https://on.ft.com/35me5Du.
[24] Kiesel, R., A. Fr hlich, S. Christ, and F. Jansen, 2020, "Russische Hacker könnten Justizdaten gestohlen haben," Der Tagesspiegel, January 28, https://bit.ly/3v8l1xB.
[25] https://bit.ly/3v5G1Gr.
[26] FACT SHEET: Biden-Harris Administration bringing semiconductor manufacturing back to America," The White House, January 21, 2022, https://bit.ly/3h7Da7G; 27; Congressional Research Service, 2021, "U.S. export control reforms and China: issues for Congress," January 15, https://bit.ly/3s7pe3D.
[28] See for President Trump's Executive Order 13959.pdf (treasury.gov) (https://bit.ly/3BHrvpJ); this EO is basically replaced by President Biden's EO, see next footnote.
[29] FACT SHEET: Executive Order addressing the threat from securities investments that finance certain companies of the People's Republic of China, The White House, June 3, 2021, https://bit.ly/33GprBz.
[30] https://nyti.ms/3LKjvbU.

Giving in to U.S. pressure will potentially in turn lead to further Chinese pressure on European governments, including threats of Chinese import restrictions on European equipment and products. This ultimately affects our digital sovereignty and makes it more urgent for us to develop our own offerings as well.

2.4 Data as a weapon

Concerns of the U.S. and China go beyond ICT-supply chain dependencies and extend to what their adversary can do with information about their companies and citizens.[31] By now, both consider access to each other's data a matter of national security (they consider data as a weapon).

Increased tensions were kicked off by President Trump banning popular Chinese apps – such as TikTok and WeChat – from the U.S. app stores because these would undermine the "national security, foreign policy, and economy" of the U.S.[32] The measures were announced as the necessary protection of U.S. citizens from the unbridled collection of their data by the Chinese government. The U.S. was not alone, the Indian government also announced its intention to ban large number of Chinese consumer apps, including TikTok, because they are a "threat to sovereignty and integrity" and undermine "national security".[33] Trump's ban on these Chinese apps was met with severe skepticism about his true motives; the ban was considered part of the trade war with China, more than based on true concerns about privacy of U.S. citizens. However, subsequent reports about the massive mining by China of Western social media data to equip its government agencies, military, and police with information on foreign targets, should also give us pause.[34] President Biden dropped President Trump's Executive Orders banning Chinese apps, only to replace them by an Executive Order that provides powers to protect sensitive data of U.S. citizens from foreign adversaries.[35]

In response, in November 2021, China issued two pieces of sweeping privacy legislations, both basically banning all exports outside China of "important data," being any data that may endanger national security or public interests. Reviewing the categories of data caught by this definition shows that it is difficult to envisage what data could still be exported (e.g., covered are already personal data relating to more than 100,000 citizens). More telling is the fact that China is even willing to crack down on its own tech companies in order to prevent data of Chinese citizens ending up in the U.S. In June 2021, when Didi, the Chinese equivalent to Uber, got listed on the New York Stock Exchange, Chinese regulators retaliated by banning the Didi app from the Chinese app stores, alleging that Didi was illegally collecting users' persona data. Didi is now in the process of shifting its shares from New York to Hong Kong, caught between China announcing stricter control over foreign listings of Chinese companies and the U.S. Securities and Exchange Commission (SEC) finalizing rules empowering U.S. regulatory authorities to delist Chinese companies if their auditors refuse to share information requested by them.

Note that concerns about large scale harvesting of social media data extend beyond individual privacy of citizens, they also concern protection of our collective data. Analysis of data of a large enough portion of a population will be predictive for the entire population. The E.U. General Data protection Regulation (GDPR), will, therefore, provide no protection here. For example, if sufficient E.U. citizens provide consent for analysis of their DNA by a Chinese company, this will potentially impact us all.

Concerns about the Chinese harvesting of social media data (via apps like TikTok) become more understandable when one considers that hereditary data (from DNA) can now be combined with socioeconomic data (information about how we live, what we eat, when we exercise and sleep). With information about heredity and environment, suddenly precision medicine will be possible, potentially bypassing doctors. China itself is well aware of the risks, and clamped down on any access to their biological data and samples.[36] Note that where both the U.S. and China limit data transfers, data exchange by the E.U. is increasingly becoming a one-way-street. In response, we see data localization requirements creeping in at, for example, the E.U. standard setting level for cloud services[37] and data export restrictions on non-personal data under in the draft E.U. Data Act (stricter even than under the GDPR for personal data).[38]

[31] Reich, R., 2021, "Data, not arms, the key driver in emerging US-China cold war," The Guardian, July 10, https://bit.ly/3BEydwx.
[32] Executive Order on addressing the threat posed by TikTok – The White House (archives.gov), August 6, 2020 (https://bit.ly/3LRNzlZ); New York Times, 2020, "Trump's attacks on TikTok and WeChat could further fracture the internet," September 18, https://nyti.ms/3sUMtxj.
[33] https://bit.ly/3H9xch8 34 https://bit.ly/3h620cX; https://bloom.bg/3h6k7dP. 35 https://bit.ly/3sYaYJR.
[34] https://bit.ly/3h62OcX; https://bloom.bg/3h6k7dP. 35 https://bit.ly/3sYaYJR.
[35] https://bit.ly/3sYaYJR.
[36] https://bit.ly/3BD4AvD.
[37] See Position Paper of the Dutch Online Trust Coalition on regulatory developments at ENISA originating from the Cyber Security Act, https://bit.ly/33lyB0y.
[38] Which is scheduled to be officially published on 23 February 2022; see for the leaked version: https://bit.ly/3h9LHXD.

EXAMPLE: CONCERN ABOUT CHINA HARVESTING BIOLOGICAL DATA

In January 2021, it was widely reported in the U.S. media that at the outbreak of the pandemic, the world's largest biotech firm (based in China and with strong ties to the Chinese government) made an offer to the governors of six U.S. states to help build and run state-of-the-art COVID-19 testing labs against very favorable conditions.[39] So favorable indeed, that it seemed like an offer the states could not refuse. When the governors compared notes, however, they concluded that some offers are indeed too good to be true, the ulterior motive of the offer likely being to obtain biometric information of large parts of the American population to be used for Chinese DNA science, to develop vaccines and precision medicine. The offer lead U.S. officials to issue public warnings to hospitals and governmental agencies that "Foreign powers can collect, store and exploit biometric information from COVID tests."[40] The Chinese quest to control biodata and therewith control healthcare's future, is also called the new space race.

2.5 Referees do not win the match

The E.U. is behind in innovation, especially in AI innovation.[41] This is due to a lack of investment, but also because for a long time Europe thought that its laws and regulations would protect it. Until as recently as 2017, talking about European sovereignty was very much not done and Europe was in favor of the open liberal market economy and European research programs, for example, had to be "open to the world".[42] Europe trusted its regulatory power to protect E.U. values and the fundamental rights of its citizens. An example is the GDPR, the world's first sweeping omnibus law protecting the personal data of individuals. In a similar vein, the E.C. intends to be the first to issue omnibus AI regulation.[43] For a long time this has been a successful recipe, the E.U. is by now considered a regulatory powerhouse, where E.U. regulations have a strong effect also outside the E.U. (coined the Brussels Effect).[44] Case in point is again the GDPR. By now about 120 countries have followed suit and adopted omnibus data protection laws, of which 17 have explicit GDPR-like legislation.[45] There is even a call by leading tech companies to make GDPR the "law of the world".[46] Though successful from a regulatory perspective, the realization has set in that GDPR may succeed in protecting data of individual citizens, but not in protecting the E.U.'s economic ecosystem. GDPR actually hampers innovation. To start with, the rules are so strict and costly to implement that they are difficult for startups and smaller companies to implement. GDPR has in practice proven to be a strong competitive advantage of large technology companies.[47] In a similar vein, the prediction is that the draft AI Regulation will be so elaborate and costly to comply with that it will likely hamper E.U. innovation.[48] Second cause is that while E.U. research is open to the world, large data-intensive companies "hide" behind GDPR so as not to open up their data for research in the public interest. And finally, and most importantly, the realization has set in that rules do not protect if you do not innovate yourself: referees do not win the match.[49] Two examples to illustrate:

2.5.1 EXAMPLE: APPLICATION OF AI

GDPR requires that deploying an algorithm should not lead to discriminatory outcomes.[50] GDPR also requires companies applying algorithms for automatic decision-making – for example, automated rejection of a loan application – to provide individuals with meaningful information about the underlying logic and an explanation of the decision, so that they can challenge the decision.[51] At present, however, advanced forms of AI are still a black box – we do not know how algorithms arrive at their outputs. Innovation is, therefore, required to prevent discriminatory outcomes and ensure transparency and explanation.[52] In fact, innovation at major U.S. tech

[39] https://cbsn.ws/34ZQGrx.
[40] Ibid.
[41] https://bit.ly/3s9NZfL; https://bit.ly/3s7VGD4.
[42] "Horizon 2020 is open to the world," https://bit.ly/3BHIND1.
[43] European Commission Proposal for a Regulation laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act), (April 21, 2021), COM(2021)206 final.
[44] Bradford, A., 2020, The Brussels effect: how the European Union rules the world, Oxford University Press.
[45] https://bit.ly/3H4Bpm5.
[46] https://bit.ly/3JM9wBe.
[47] Yueh, J., 2018, "GDPR will make big tech even bigger," Forbes, June 26, https://bit.ly/33EyXVN.
[48] MacAfee, A., 2021, "EU proposals to regulate AI are only going to hinder innovation." Financial Times, July 25, https://on.ft.com/3sX7tn4.
[49] https://politi.co/34Zi0Gm; https://bit.ly/3s895ek.
[50] We regularly see in the news that the application of self-learning algorithms leads to discriminatory outcomes, see for example: Dastin, J., 2018, "Amazon scraps secret AI recruiting tool that showed bias against women," Reuters Business News, October 10, https://reut.rs/3sX7dV8.
[51] Articles 13, 14, and 22 (3) and Recital 71 of the GDPR. For information on these requirements, see Moerel, L., and M. Storm, 2019, "Automated decisions based on profiling: information, explanation or justification, that is the question!" in Aggarwal, N., H. Eidenmüller, L. Enriques, J. Payne, and K. van Zwieten (eds), Autonomous systems and the law, C. H. Beck.
[52] It is not easy to do this properly. See Moerel, L., 2018, "Algorithms can reduce discrimination, but only with proper data," Op-ed, IAPP Privacy Perspectives, November 16.

companies is currently geared toward cracking this black box and developing new de-biasing techniques.[53] Various media reported that Google has tackled the black box problem with "explainable AI",[54] which is expected to be a major competitive advantage going forward.

2.5.2 EXAMPLE: DATA TRANSFER RULES

In terms of control over European data, worrying from a sovereignty perspective is that U.S. intelligence agencies have certain powers for espionage and counterterrorism purposes to intercept foreign data in transit to the U.S. on transatlantic cables, and also have powers to collect data from U.S. cloud providers if they are hosted on servers in the U.S.[55] Two specific interception powers[56] have recently led the European Court of Justice (ECJ) in the well-known Schrems II judgment[57] to rule that U.S. law does not provide an equivalent level of protection to personal data of European citizens after being transferred to the U.S. U.S. law does not meet the requirements of the GDPR and the European Charter of Fundamental Rights of the E.U. The judgment has far-reaching consequences because in countries such as China, Russia, and India, the authorities have similar interception powers as the U.S. authorities. Also for these countries, data transfers are, therefore, under discussion. The ECJ leaves open the possibility for organizations to take supplementary mitigating measures that in specific cases address the shortcomings as a result whereof transfers can still take place.[58] Since U.S. intelligence agencies are not bound by contractual measures between the data exporter and importer, an obvious solution is to seek additional protection in data encryption. The data can then still be intercepted, but the foreign states can do little with these. Fact is that currently encryption is only possible for data at rest and for data in transit. Here too we see technical innovations in which data in use can also be encrypted (so-called homomorphic encryption).[59] U.S. cloud providers are the first to come up with practical applications here.[60] This form of encryption ensures that U.S. intelligence services do not have access to identifiable data, even when obtained when the data were in use. At the same time, it ensures that the providers themselves can analyze the data in order to generate insights. This innovation will, therefore, further strengthen the dominant position of these providers (see next section).

DATA CAN BE IN THREE STAGES:

Data at rest: the data are inactive and stored, for example in a database.

Data in transit: the data are transported over a network.

Data in use: the data are processed in an application.

Homomorphic encryption is a form of encryption that allows operations to be performed on the data without first having to decrypt it.

Exit and transition: customer dependencies often arise when contracts terminate because the customer needs the cooperation of the supplier for the transition of data and applications to a successor supplier (who in turn applies its own standards). For this purpose, specific protocols for "exit and transition" are already agreed upon at the conclusion of the contract.

2.6 Dependencies on dominant foreign suppliers

It will require little explanation that where governments and providers of critical infrastructure increasingly outsource their ICT systems, data storage, and processing to suppliers, new dependencies arise, especially if those suppliers are dominant market players.[61] The concept of digital sovereignty then also extends to the autonomy of our government and providers of critical infrastructure vis-à-vis these commercial parties, and where these are foreign parties, to their respective governments.

[53] The U.S. government is also making an effort. See, for an example of innovation in the field of explainable AI (also known as XAI), a project by the Defense Advanced Research Projects Agency (DARPA), Gunning, D., "Explainable Artificial Intelligence (XAI)," https://b.gatech.edu/3BHGVtZ.
[54] Kelion, L., 2019, "Google tackles the black box problem with Explainable AI," BBC, November 24, https://bbc.in/3p7DUhl.
[55] For a (still up-to-date) overview of the possibilities of interception by U.S. intelligence services of data of non-Americans, see Gorski, A., 2018, "Summary of U.S. Foreign Intelligence Surveillance Law, practice, remedies and oversight," American Civil Liberties Union Foundation, August 30, https://bit.ly/3JBHt7s.
[56] This concerns the powers of U.S. intelligence agencies under Section 702 of the Foreign Intelligence Surveillance Act ("FISA") and Executive Order ("EO") 12333.
[57] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd, ECLI:EU:C:2020:559 (July 16, 2020), https://bit.ly/3BEB4FR.
[58] Ibid, See paragraph 133.
[59] See on this topic: Divatia, A., 2019, "Fact and Fiction of Homomorphic Encryption," Dark Reading, January 22, https://bit.ly/3p3aWzq.
[60] See for offer Microsoft: https://bit.ly/3v6oOwm; IBM: https://ibm.co/3BHVL3q, and Google: https://bit.ly/35jrcVW.
[61] The Dutch Scientific Council for Government Policy, in its advice "Preparing for digital disruption," 2019, Chapter 3, gives a good overview of the far-reaching digitalization of society, the strong interweaving of the digital domain and the physical domain, and the new vulnerabilities that this creates for core societal processes, WRR Advice Digital Disruption, https://bit.ly/34ZCbnx.

The international cloud providers compete on security and are best in class. The deployment of cloud solutions now offers so many advantages in terms of functionality (e.g., built-in data analysis tools), higher implementation speed, innovation, the possibility of collaboration, and often lower costs, that the use of cloud services is now also seen as "necessary for a well-functioning government", making government policy cloud first, both in the Europe as in member states.

In the market, there is a very limited choice of so-called hyperscalers (cloud providers with large capacity). As a consequence, currently 92 percent of the data of European companies and citizens reside in the clouds of U.S. technology companies, of which 80 percent are with five providers only.[62] European suppliers hardly appear in the picture.[63] These five players are now so big that if there is an outage of one of them, it is like a power cut, entire E.U. sectors will be down. If 10 years ago we would have asked ourselves whether this – in principle – would be a good idea, none of us would have answered in the affirmative. We would never put the switch of our power grid in the hands of a foreign company, and its government.

The dominance in market positions further leads to an imbalance between supplier and customer, with monopolistic behavior in contracts, price, service, and dependencies for the future (not only because of dependencies on contract termination (exit and transition), but also because making changes to standard solutions is difficult).[64]

The major market players offer limited interoperability and portability of data and applications. Because of their scale, they are able to use their own standards – often protected by intellectual property rights – and even to build a private internet infrastructure (including even their own submarine cables),[65] which makes them virtually autonomous both physically and legally and makes any interconnection difficult, both in terms of infrastructure and data exchange.[66] To prevent vendor lock-in, clients (including governments)[67] usually have a so-called multi-vendor strategy. However, under current market conditions, this is difficult to achieve.

The current expectation is that – without government intervention – the dominant positions of these market players will only increase. These market players are systematically expanding their ecosystem by integrating new functionalities into their services (such as cybersecurity and data analysis tooling), which will only increase vendor lock-in.[68] They are also able to attract the best talent worldwide and have almost inexhaustible access to capital. This enables them to continuously monitor innovations and startups, which they then take over at an early stage and integrate into their own offerings.[69]

These dominant positions (winner takes all) are a sign of the times and should not be taken as a given. As said, our society is undergoing a technological revolution, which brings along disruption and friction. History shows that whenever new technologies disrupt society, it needs time to adjust and regulators always play catch-up. At this time, the digital society is still driven by the possibilities of technology rather than social and legal norms.[70] These frictions will ultimately be addressed. For example, the first industrial revolution brought child labor, abuse of workers, and the skies of London were so full of soot that people fell ill. The barons of the new industry (steel, oil, copper, and coal) reigned supreme, with worsening inequalities due to their monopolist positions. Ultimately many new laws were introduced, most notably the first antitrust regulation, which broke up the monopolies. Illustrative here is that President Biden, when introducing his Executive Order on Promoting Competition in the American Economy,[71] made several references to the importance of abiding to the original principles of antitrust regulation also in the new digital economy: "It is the policy of my Administration to enforce the antitrust laws to meet the challenges posed by new industries and technologies, including the rise of the dominant Internet platforms, especially as they stem from serial mergers, the

[62] Amiot et al. (2020).
[63] Synergy Research Group, October 29, 2019.
[64] European Commission, 2020, "Communication: a European data strategy," February 19, https://bit.ly/3BJyYV1.
[65] Where even own submarine cables are laid, see for Google: https://bit.ly/34ZBmLt; and for Microsoft and Facebook: https://bit.ly/3v8RG7s.
[66] See farewell speech Jan Smits, https://bit.ly/3v8oBZy.
[67] See e.g., Cloud principles JenV, p.2, and European Commission/DIGIT (Appendix 3 – EU Cloud Policy).
[68] This problem is also called out by the European Commission, See European Data Strategy, p. 7. The financial sector (banks, supervisory authorities, etc.) also analyzes the strategic aspects of its own cloud policy. The European Securities and Markets Authority (ESMA) opened the consultation of its directive on cloud outsourcing on June 3. Steven Maijoor, the chairman of ESMA, explained, "Financial markets participants should be careful that they do not become overly reliant on their cloud services providers. They need to closely monitor the performance and the security measures of their cloud service provider and make sure that they are able to exit the cloud outsourcing arrangement as and when necessary." https://bit.ly/3JNPZjY.
[69] See about these practices: https://bit.ly/36INAhI.
[70] Moerel, L., 2014, "Big data protection: how to make the draft EU regulation on data protection future proof," working paper, Tilburg University, https://bit.ly/3JQs5Et.
[71] https://bit.ly/3s72nFC.

acquisition of nascent competitors, the aggregation of data, unfair competition in attention markets, the surveillance of users, and the presence of network effects."

My point here is that governments around the world (including the U.S., China, and the E.U.) are currently considering their policy responses and antitrust investigations are underway on all continents.[72] Once these have done their work, the world will look very different indeed.

3. E.U. POLICY RESPONSE

An important upfront observation is that the E.U.'s mandate to safeguard the necessary form of sovereignty is limited. Although the E.U. can take initiatives in a large number of areas to strengthen "digital sovereignty", there is an important obstacle. In essence, the problem is that digital sovereignty soon touches on the national security of member states, which under the E.U. treaties is the prerogative of the member states. Where, however, the member states individually can no longer protect their sovereignty, the limited European mandate actually undermines national security.[73] E.U. digital sovereignty policy is, therefore, often framed in terms of the power of the E.U. to regulate the "internal market", while the real underlying denominator is protection of sovereignty. Where previously this would raise concerns among member states, we see an increased willingness to cooperate at the European level in the digital domain and to pool or share sovereignty.[74]

The second observation is that due to the multifaceted nature of the causes of the pressure on our digital sovereignty, there is no one-size-fits-all solution. Europe's sovereignty will have to be supported by a "smart" combination of measures acknowledging that becoming self-sufficient is not realistic for Europe, but also not desirable.[75] With the E.U. policy measures, the E.C. is aiming to pave a third way, aiming to avoid falling into the trap of tech protectionism. The policy is, for example, not to exclude foreign digital providers, nor for Europe to build its own hyperscalers. And rightly so, if you have concerns about vendor/data lock-in with current big tech companies, you will have similar concerns with their E.U. equivalent. Rather than blocking foreign suppliers, E.U. policy is about breaking through vendor/data lock-in by ensuring:

- **Interoperability of cloud infrastructure** in order to achieve the required scalability for innovations, without setting up its own hyperscalers.
- **Open data**, which makes it possible for an industry sector to combine its data in a common data space, to unlock their value for AI innovations.
- **Open source technologies**, which can be worked on collectively, and forked individually; the only way Europe will be able to match the R&D budgets of the tech giants, gaining both the benefits of scale and self-sovereignty.[76]
- **Federated solutions**, whereby data are not continuously copied, but remain at the source and are drawn on, where necessary, preserving privacy and self-sovereignty.

3.1 Increased cyber resilience and regulation of gatekeepers

Important building blocks of the E.U. sovereignty policy measures (but not further discussed here) are omnibus measures to increase the cyber resilience of critical infrastructures and services in Europe in the upcoming directive on the resilience of critical entities and the renewed Security of Network and Information Systems (NIS2) Directive.[77] Other components are proposals to better regulate the market power of gatekeepers providing core platform services (such as search engines, social networks, video sharing, and cloud computing services) in the Digital Markets Act[78] and increased requirements and liability of large online platforms related to the spreading of illegal content, misinformation, and targeted advertising practices in the Digital Services Act.[79]

[72] See for overview: https://bit.ly/3h62B9D.
[73] See on this paradox and potential solutions, Timmers, P., and L. Moerel, 2020, "Reflections on digital sovereignty," E.U. Cyber Direct, January 15, https://bit.ly/3s7sz2K.
[74] A telling example is 5G security, where the Member States asked the EC to draw up a joint direction for 5G security, even though the concerns in this area primarily concern national security. This was unthinkable not so long ago.
[75] See Timmers and Moerel (2020) for three approaches to achieve digital sovereignty: risk management, strategic partnerships, or working together on a global level to find solutions in the common interest (global common goods).
[76] Thompson, B., 2021, "Internet 3.0 and the beginning of (tech) history," Stratechery, January 12, https://bit.ly/3sag1Ib.
[77] European Commission, 2020, "Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive," (E.U.) 2016/1148, December 16.
[78] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final.
[79] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final.

3.2 Open data – open infrastructure – open source

The focus here is on the other policy initiatives – all dating from 2020 – and aimed at ensuring interoperability of E.U. data and cloud infrastructure, avoiding vendor/data lock-in.

3.2.1 OPEN DATA

The cornerstone is the E.U. Strategy for Data,[80] and specific for the financial sector: the E.U. Retail Payment Strategy[81] and the Digital Finance Strategy.[82] The European Strategy for Data aims to democratize access to data assets and drive data sharing in open digital ecosystems across the whole economy. It also aims to create a single market for data to be exchanged across sectors efficiently and securely within the E.U. in a way that fits European values of self-determination, privacy, transparency, security, and fair competition. The centerpiece of the European Data Strategy is the concept of European data spaces, bringing together E.U. data of nine defined clusters of organizations with common interests (including financial, health, and government), so that the scale of data required for innovation for a cluster can be achieved. The design of the data spaces will be based on full interoperability and data sovereignty, whereby users will be provided tools to decide about data sharing and access.[83] With the actual parties that generate the data regaining control, large hyperscalers will no longer be able to achieve vendor/data lock-in in their proprietary ecosystems. In this context also fits the Data Governance Act,[84] opening up public data for innovation through independent intermediaries and the draft E.U. Data Act, providing a harmonized framework for all data sharing, conditions for access by public bodies, data export restrictions for non-personal data, and portability and interoperability requirements for cloud services.[85] Where data spaces require many-to-many interactions, digital identity solutions and consent dashboards will become an inherent part of the design (E.U. digital identity solutions are further discussed in section 3.3, below).

3.2.2 OPEN INFRASTRUCTURE

Another flagship initiative is the GAIA-X project,[86] which is aimed at achieving interoperability between cloud offerings to achieve the required scalability of the cloud infrastructure for AI-related innovation, not by creating Europe's own vertical hyperscalers but by networking (making interoperable) the current European offer of cloud infrastructure, enabling clients to scale up within that network (i.e., scaling up in a horizontal way). This is achieved by setting common technical standards and legal frameworks for the digital infrastructure and standardizing contract conditions. This form of interoperability goes beyond portability of data and applications from one vendor to another to prevent vendor lock-in; it really concerns the creation of open APIs, interoperability of key management for encryption, unambiguous identity, and access management, etc. Cloud providers will be expected to offer a choice as to where (personal) data are stored and processed, without otherwise requiring storage in Europe. The GAIA-X project is not a comprehensive European policy, but it is a concrete realization of the open interfaces, standards, and interconnection needed for the European policy and explicitly based on principles of sovereignty-by-design. The project is open to foreign suppliers as long as they embrace the principles. From a digital sovereignty perspective, the GAIA-X project is a logical and promising initiative and is gaining more and more traction.[87] The expectation is that once the design principles are agreed upon, these may well become mandatory for all cloud services in Europe. Some of the elements (portability and interoperability requirements and data export restrictions for non-personal data) are already included in the draft E.U. Data Act.

Though the initial aim of GAIA-X is to achieve an open cloud infrastructure in an open market, we have recently seen that digital sovereignty concerns lead to an increased pressure to move to stand-alone E.U. cloud only solutions, whereby all E.U. data are stored in the E.U. only (unless the service requires transfer of data, e.g., in case of communication services). Rather than addressing sovereignty concerns in respect of

[80] European Commission, 2020, "A European data strategy," COM(2020)66, February 19.
[81] European Parliament, 2020, "Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions on a Retail Payments Strategy for the EU," https://bit.ly/3v3ZhnH.
[82] European Parliament, 2020, "Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions on a Digital Finance Strategy for the EU," https://bit.ly/3BOdxSY.
[83] See for overview of the data space design principles: "Design principles for data spaces," position paper, https://bit.ly/3p79v2O. 84 Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final.
[84] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM/2020/767 final.
[85] Which is scheduled to be officially published on 23 February 2022; see for the leaked version: https://bit.ly/3t4ExcC.
[86] "A Federated data infrastructure as the cradle of a vibrant European ecosystem," the GAIA-X project initiated by the German and French governments, October 2019, based on principles of sovereignty-by-design.
[87] In the Netherlands, a coalition of TNO and a number of industry associations are actively contributing to the GAIA-X project, https://bit.ly/3p7hbSx.

foreign cloud providers and data transfer issues at an E.U. policy level, we see data localization requirements creeping in at, for example, the E.U. standard setting level for cloud services[88] and data export restrictions on non-personal data under in the draft E.U. Data Act (stricter even than under the GDPR for personal data). Telling in this context is that Commissioner for the Internal Market Thierry Breton recently stated: "European data should be stored and processed in Europe because they belong in Europe."[89] It is not clear yet what the end result will be.

3.2.3 OPEN SOURCE TECHNOLOGY

The E.C. has an active open source software strategy, where open source solutions are preferred when equivalent in functionalities, total cost, and cybersecurity,[90] which facilitates decentralized and federated services that can be independently audited, contributing to public trust. Open source technologies can further be worked on collectively, which provides benefits of scale (combining the E.U. R&D to potentially match the R&D budgets of the big tech companies), but also ensures self-sovereignty as open source can always be subsequently forked individually for specific solutions.[91]

3.3 E.U. digital ID wallets

Part of the policy package is a proposal to create a modernized framework for a European digital identity,[92] based on self-sovereignty of European citizens. Member states will offer citizens and businesses "European digital ID wallets"[93] (digital ID wallets), which are stored as an app on smartphones and enable E.U. citizens to authenticate and access online services across the E.U. The digital ID wallets will be issued by a member state or by private entities (after their wallet is certified by accredited bodies designated by the member states). The digital ID wallets will enable citizens to do more than simply prove their identity: the wallets will also store proof of other personal attributes and credentials, such as driving license, education certificates, birth certificate, bank cards, a specific attribute to demonstrate you are older than 18 (to access certain websites), and further enable citizens to digitally sign documents with a qualified electronic signature (this is a higher level of identity proofing and security and is suited for banking transactions). This will be a big change. For example, when renting a car, an individual can prove possession of a driving license by sharing the attribute "in possession of a driving license" from the digital ID wallet, without having to actually provide a copy thereof. At the moment, citizens still have to login for each and every digital service with the vulnerable system of user name combined with password and manually enter and disclose (always the same) personal data. To simplify login, many websites offer citizens the option to authenticate via their account with one of the major foreign platforms, such as Facebook, Google, and Alibaba. This creates large concentrations of both business and personal data on these platforms, which has a direct impact on citizens' privacy and digital sovereignty.

Under the new regulation, large platforms will be required to accept the use of the digital ID wallets as well as all services that require strong customer authentication (SCA). The new regulation further restricts sharing of personal data to what is strictly necessary for the provision of the service, precludes the issuer of the wallet from collecting information on the use of the wallet, and prevents the issuer from combining personal data in the wallet with any other personal data in its possession, "unless the citizen expressly requested it".

Where data sharing across industries (in a so-called multi-to-multi-markets) becomes the norm, digital ID wallets will become a new intermediary function in the ecosystem, potentially disrupting current platforms. Not surprisingly, Apple has already included self-sovereign wallet functionality in its latest iOS 15, which may well meet the E.U. requirements.[94] The Apple ID wallet will be disruptive for the other large platforms (as these once were to others) and is expected to become its next big revenue source, more so than Apple Pay.[95]

Though the above restrictions on data collection and combining by issuers of the wallet may – at face value – seem detrimental to digital business models of issuers, the opposite

[88] See Position Paper of the Dutch Online Trust Coalition on regulatory developments at ENISA originating from the Cyber Security Act, https://bit.ly/3saeSQT.
[89] According to a POLITICO interview on September 1, 2020, https://politi.co/3JJJQoS.
[90] Communication to the Commission Open Source Software Strategy 2020 – 2023 Think Open, C(2020)7149 final, https://bit.ly/3BNhozx.
[91] https://bit.ly/3H8tZ1q 92 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (E.U.) no. 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final.
[92] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (E.U.) no. 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final.
[93] Defined in Article 3(42) as "a product and service that allows the issuers to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals."
[94] Velasco, J., 2021, "Apple wallet with iOS 15 is close to replacing your wallet," Digital Trends, June 7, https://bit.ly/3sX2see; Apple, 2021, "Apple announces first states to adopt driver's licenses and state IDs in Wallet," press release, September 1, https://apple.co/3JIxnBI.
[95] https://bit.ly/3JIxehE.

is the case. Where many market players have to accept the digital ID wallet for authentication, having the channel to actually be able to request consent from users for data sharing becomes a competitive advantage in and of itself.

3.4 Impact on financial sector

Looking at these policy initiatives, these will have a fundamental impact also on the business models of the financial sector. The introduction of "open banking" in the revised Payment Services Directive (PSD2) and the E-Money Directive already lowered the barriers for non-banks (fintechs, big tech, etc.) to leverage the payment data of banks in order to provide value propositions on top of the payment infrastructure.[96] Financial institutions also complain that there is an increased use of the authentication solutions of big tech companies to access their payment processes, increasing their dependency on these providers and making it difficult to maintain the security of access to their services. In fact, banks complain about the gatekeeper function of big tech. However, due to the E.U. policy measures, what really is at stake is the banks' own gatekeeper function: "banks are no longer the sole manufacturers and distributors of payments and other financial products (e.g., loans) and hence risk losing their long-held dominance of the sector."[97] As often, once the insight is there, regulatory changes are also an opportunity. Instead of resisting the open banking and open data requirements, banks are well advised to embrace these and become open banks, facilitating (also) data driven transactions and many-to-many reach, for example, by allowing consumers to share energy data with loan providers.[98] As already well described by other authors, in this new data ecosystem banks could well leverage their customers' trust (and preserve customer contact and relevance) by becoming digital identity providers and data custodians.[99] As indicated above, digital ID wallets will quickly become a new intermediary function in the ecosystem, disrupting the gatekeeper function of the current platforms. The restrictions on issuers of wallets as to data collection and combining may seem detrimental, but actually create a channel to request consent from users in the first place (preserving customer contact and relevance).

The adoption of digital ID wallets will further accelerate digitalization in and of itself, e.g., will enable banks to rely on these digital identities to perform know your customer/anti-money laundering (KYC/AML) due diligence, facilitate executing banking documents, and use these identities to meet strong customer authentication (SCA) requirements under the revised Payment Services Directive (PSD2). Taking it one step further, banks could also become an active attribute provider for wallets, such as KYC/AML attributes, which can also be used by other service providers (against a payment). This will enable the banks to actually monetize their current KYC/AML efforts. Rather than frowned upon, this is actively encouraged by the E.C.[100] Other relevant attributes to be issued by banks could be source of funds, source of wealth, insolvency/bankruptcy risk, transactional behavior, banking relationship, etc. Where the European Central Bank is working towards a digital euro,[101] the digital ID wallet should in the future also facilitate payments with these digital currencies (digital currency wallet), including complex transactions like cross-border or multi-currency transactions. In this last scenario, all features of the E.U. digital policy will be combined: open banking, digital currency, digital ID wallets, and SCA under PSD2.[102]

4. CONCLUSION

History shows that whenever new technologies disrupt society, it needs time to adjust and regulators always play catch up. At this time, the digital society is still driven by the possibilities of technology rather than social and legal norms. This inevitably leads to social unrest and calls for new rules. An illustrative example here is that in 2010, Mark Zuckerberg (CEO and founder of Facebook (Meta)) caused quite a stir when he publicly announced that the end of privacy was in sight: "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time."[103]

[96] Zachariadis, M., and P. Ozcan, 2017, "The API economy and digital transformation in financial services: the case of open banking," SWIFT Institute working paper no. 2016-001, https://bit.ly/3lf1vUY.

[97] Cortet, B., M. Bakker, P. Groen, and D. Hoppenbrouwer, 2021, "Establishing the trust anchor in the digital economy: The case for banks to become 'data custodians,'" Journal of Payments Strategy & Systems 15:2, 150-164.

[98] Ibid.

[99] World Economic Forum, 2016, "A blueprint for digital identity, the role of financial institutions in building digital identity," https://bit.ly/3BOaGcl; Wilson, M., 2021, "Commercialising open banking – digital identity, a key opportunity for banks?" https://bit.ly/3s8OeaP.

[100] https://bit.ly/3p5WAOO.

[101] Wagner, E., D. Bruggink, and A. Benevelli, 2021, "Preparing euro payments for the future: a blueprint for a digital euro," Journal of Payment Systems & Strategies 15:2; European Central Bank, 2021, "ECB publishes the results of the public consultation on a digital euro," press release, https://bit.ly/34X9pUA.

[102] Adams, M., L. Boldrin, R. Ohlhausen, and E. Wagner, 2021, "An integrated approach for electronic identification and central bank digital currencies," Journal of Payment Systems & Strategies 15:3.

[103] Johnson, B., 2010, "Privacy no longer a social norm, says Facebook founder," The Guardian, January 11, https://bit.ly/3p60fw0.

However, in March 2019 (following the Cambridge Analytica data analysis scandal), Zuckerberg requested that the U.S. senate regulate tech companies[104] and further announced a complete overhaul of Facebook's privacy features: "The future is private... and that's the next chapter for Facebook."[105] From privacy is dead to privacy is the future. My point here is that not only are technical developments moving fast, but also that social standards and customer expectations are evolving and that it will take years before we will have a somewhat clear and predictable new regulatory framework.

The threats to E.U. digital sovereignty have led to a flurry of E.U. digital policy measures, that will disrupt the digital landscape as we know it by working towards open infrastructure, open data, and application of open source technology. E.U. digital policy will have a fundamental impact on the business models of the financial sector. When E.U. policy has done its work, the world will look very different, though how it will look is anyone's guess. The financial sector has to be well tuned in to these developments to determine a digital strategy that can benefit from the new reality. Digital is not a communication channel or a specific expertise, it is, by now, the business itself. It is not possible to manage a company without knowledge of the business. For those tuned in, the E.U. digital policy may bring new requirements, but first and foremost many opportunities for innovation.

[104] Miller, J., 2019, "Mark Zuckerberg asks governments to regulate tech firms," Techspot, March 31, https://bit.ly/3vctrFk.
[105] See videos at: Hassan, A., 2019, "Zuckerberg promises 'complete overhaul' of Facebook geared towards user privacy at F8," ABC, April 30, https://abc13.co/3lhJBkC.

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy specializing in driving digital transformation in the financial services industry. With a growing client portfolio comprising of over 100 global organizations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to deliver end-to-end data-driven solutions and fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its Innovation Labs and award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Twitter, Facebook, YouTube, LinkedIn Instagram, and Xing.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company