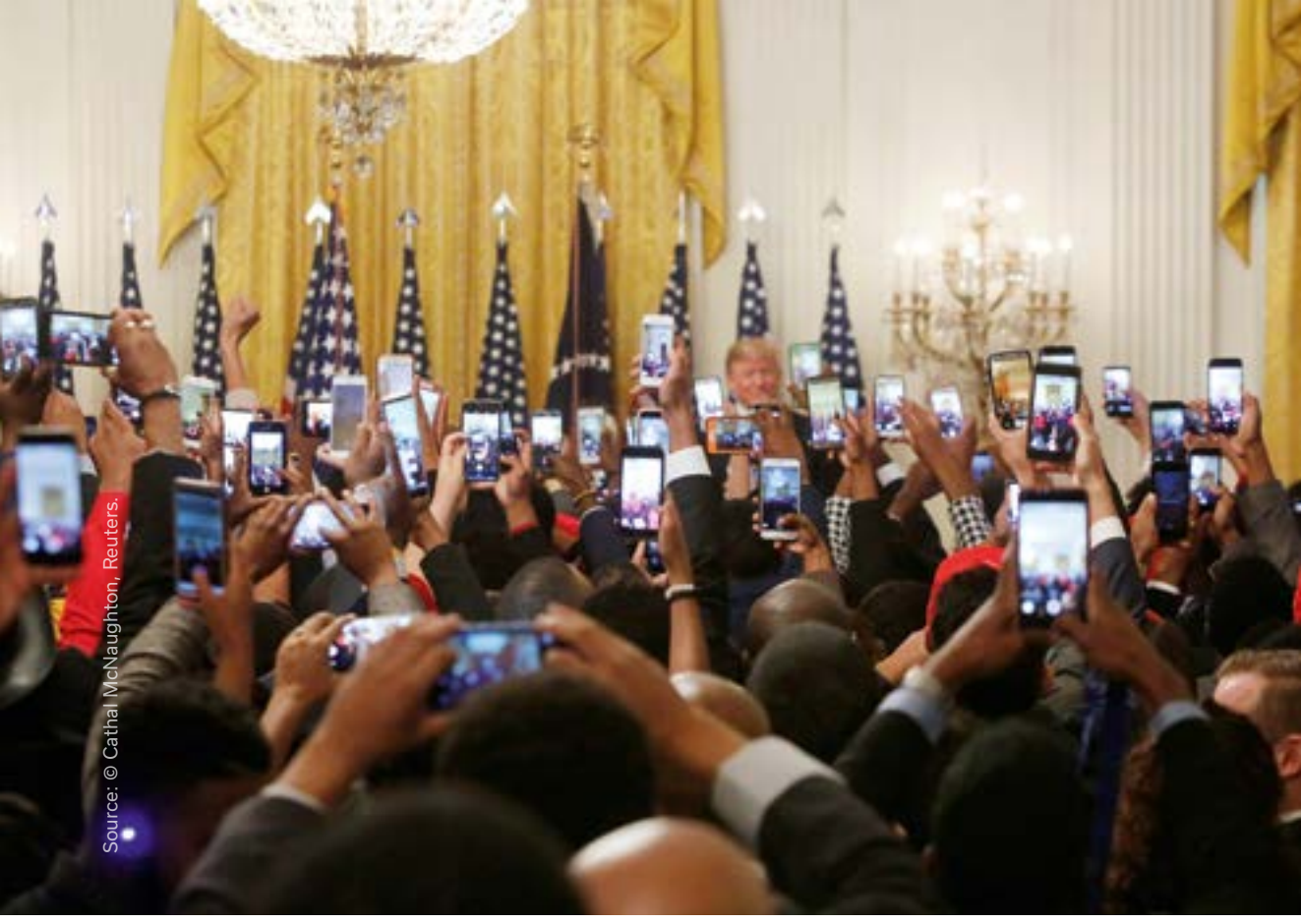


Source: © Cathal McNaughton, Reuters.

Looking West

# Between Innovation and Regulation

## The Necessity of Transatlantic Cooperation in the Digital Sphere

Sebastian Weise

The digital revolution is already increasingly impacting business and our daily lives, and fuels an accelerating process of transformation in Western societies. Due to its power to drive innovation, many people believe that shaping this digital transformation is not only an urgent endeavour, but perhaps the endeavour of our time. The digital revolution is a global process that does not stop at national borders, so configuring its future requires cross-border responses. This article looks at the role that the transatlantic alliance can and should play in this endeavour.

## Ensuring the Economic Success of the Digital Revolution Requires Transatlantic Responses

If we look at the figures on transatlantic trade, the digital economy, and data flows we see that the US and Europe are closely interwoven markets and data spheres that drive each other's economic growth. As the world's two largest economic areas, Europe and the US are each other's main trading partners and today the majority of global data flows between the two.[1] It is precisely this free flow of data that enables the current volume of transatlantic trade in goods and services as well as boosting economic growth in general.[2] Transatlantic trade is particularly strong in the digital economy, eclipsing trade relations with other continents.[3] This is important because the digital economy is a key element of economic growth and a driver of innovation, something that is vital for Europe's economic clout in the future.[4] The digital economy is also an area where the US has a trade surplus with Europe.[5] If we look at the key drivers of digital innovation in Europe, it is clear that US technology companies in particular have set the pace in recent years. Companies, such as Google (Alphabet), Apple, Facebook and Amazon (GAFA for short), have had a significant impact on Europe's digital revolution[6] and are set to continue playing this role.[7] The US is, therefore, a key point of reference for Europe, not just *per se*, but as an economic power and driver of digital innovation. As the home of the digital pioneers, the US is an important partner and these tech companies have a special role to play in shaping the economy of tomorrow (the digital platform economy). For the US, these companies are of vital importance as drivers of innovation, while Europe is a priority as a market and data pool.

## Why Transatlantic Responses Are Needed to Ensure the Digital Revolution Benefits Society

While the end of the Cold War led some to claims that we had reached the end of history, today's Western model of liberal democracy finds itself under pressure once again. It is being challenged by a global tide of authoritarianism with China and Russia at its helm. In this clash of world orders, technology has a particularly important role to play. Authoritarian states seek to utilise digital advances to reflect their own values and worldview and to use these changing dynamics to build up their own power.

Looking back over the last twenty years, China has undergone a remarkable development to become an economic powerhouse.[8] It has recently overtaken Germany as the world's leading exporter and edged past the US in volume of world trade. Some estimates now suggest that China could become the world's largest economy in quantitative terms by the mid-2020s.[9] Going beyond that, China strives to catch up with the West in a number of key future technologies,[10] and its long-term aim is to be a global leader for innovation.[11] China is

not only investing huge sums in research and development but also using a number of illegitimate trade practices[12] in order to help it gain a global leadership role and continue its ascent as a major economic power.

In addition, authoritarian states, above all China and Russia, are harnessing digital advances to reflect their authoritarian values and worldview:[13] Internet shutdowns, massive censorship of websites, persecution/identification of political opponents via social media, the use of the latest technologies for state surveillance (face recognition), and the introduction of a social scoring system. All these are examples of how authoritarian states are using technological advances to the detriment of their citizens' civil liberties, thereby consolidating their authoritarian structures at a relatively low cost.[14]

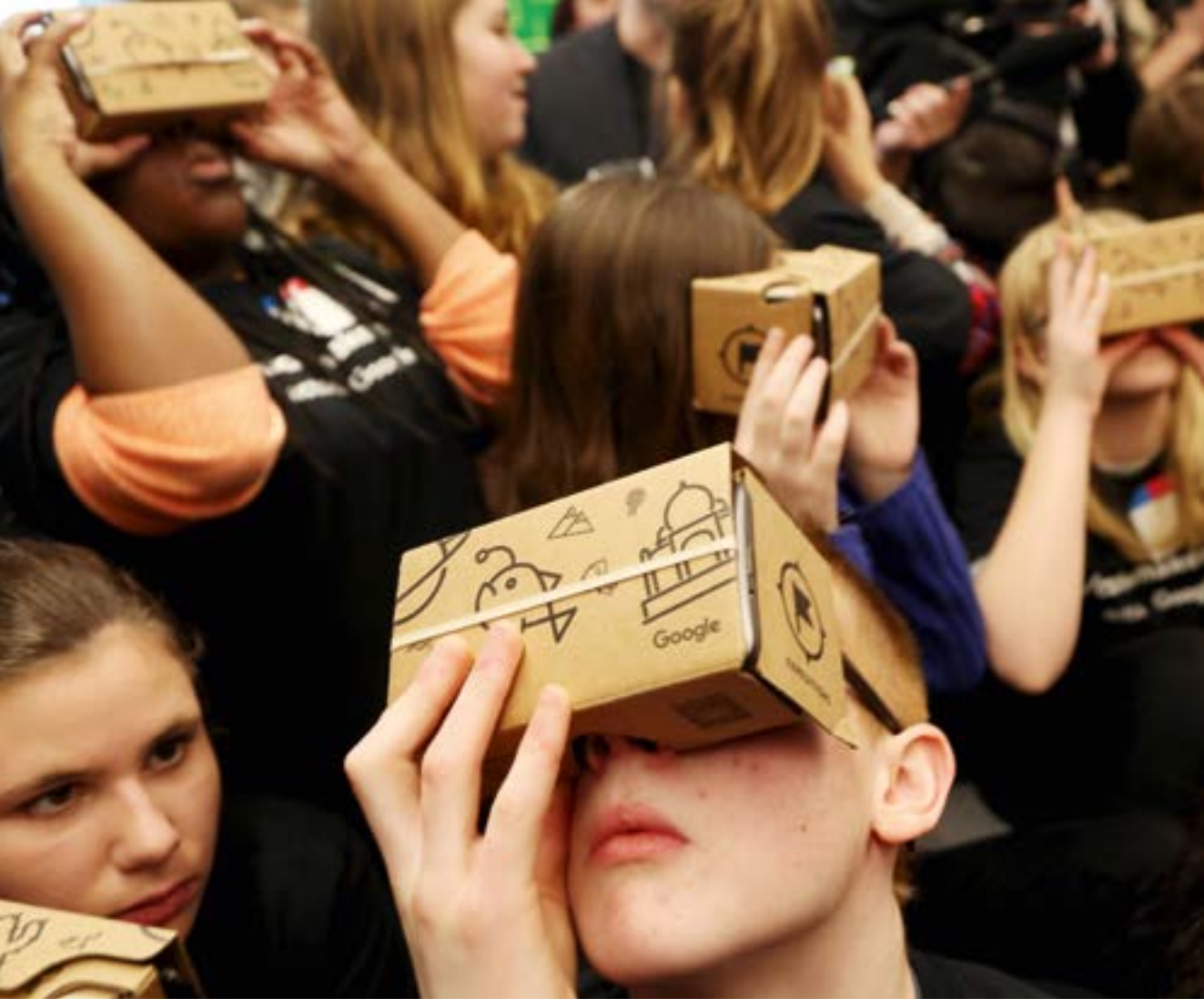
**Authoritarian regimes are using new digital technologies as part of their strategic efforts to undermine the security of Western states and their social cohesion.**

China is not only using new technology for authoritarian purposes at home, but also exporting digital authoritarianism to other countries. This was clearly illustrated by the export of surveillance technologies to Ecuador and Venezuela via the One Road One Belt project.[15] In addition to exporting technology, Russia and China are pushing for the establishment of an alternative digital world order that will further strengthen its digital authoritarianism. Rather than the liberal idea of a free and open internet managed by a multi-stakeholder model, authoritarian states advocate that the internet should be governed by a state-centric approach. This would not only make governments the central actors but, in terms of information security, they would be in a position to censor the internet within their own national borders, monitor users without judicial control, and promote the fragmentation of today's World Wide Web into national virtual spheres.[16] A plethora of cases of e-espionage, cyber-attacks, fake news campaigns and targeted attempts to influence elections via social media, coupled with the publication of compromising data, also demonstrate how authoritarian regimes are using new digital technologies as part of their strategic efforts to undermine the security of Western states and their social cohesion.

In order for liberal democracies to continue flourishing in the face of this challenge, Europe and the US need to shape digital progress within their borders to match their principles and demonstrate the superiority of the liberal world order in the competition between social systems to lead the world in innovation. At the global level, Europe and the US need to leverage technology to continue building a liberal, democratic framework for digital innovation, based on shared values and interests and with a view to curbing digital authoritarianism.

### The Origins of the Idea of Europe's Technological / Digital Sovereignty

In the past, Europe and the US had very similar interests and values with regard to digital policy. Supported by a generally optimistic "internet zeitgeist", Europe and the US worked within the framework of the Internet Freedom Agenda to seize new opportunities presented by the World Wide Web, both at home and abroad. They believed that a free and open internet would promote economic growth and innovation, improve the resilience of liberal societies and democracy itself, fuel global development, and advance the spread of human rights and democracy.[17] Many proponents of this optimistic perspective on technology viewed the Arab Spring as an important sign of the emancipatory and disruptive potential of new technology and the need to promote it based on liberal values. However, a turning point came in 2013 when Edward Snowden dropped his bombshell. This led the public to realise that technology also had its downside, and the "internet zeitgeist" lost




Restricted view: US companies such as Google have a significant impact on the digital space in Europe.
Source: © Peter Power, Reuters.

something of its appeal. The revelations about the practices of the intelligence services also made it clear that there were serious differences between the transatlantic partners. On this side of the Atlantic, there were now increased calls for Europe to have greater digital sovereignty[18] and more autonomy in shaping technological progress.[19] This desire for greater digital sovereignty has become more entrenched over recent years and is now regarded to be imperative for Europe's actions.[20] Is Europe currently facing the dual challenge of defending its economic prosperity, its values, and hence its role as a major player in shaping the digital future against the dominance of the US and China?[21]

**What Are the Main Areas of Conflict Today?**

When we look at the main areas of today's transatlantic conflict, we see that they have two main causes. Firstly, the different approaches to digital innovation in Europe and the US, and secondly a number of scandals surrounding globally operating US technology companies, which have served to increase political and public awareness of the pros and cons of digital progress. Moving on from Edward Snowden's revelations about the controversial practices of the US intelligence services, the focus has turned to data protection, liability issues related to content published on social media, taxation,

fake news campaigns and the influencing of elections. The reasons behind the USA's pronounced scepticism towards Europe's digital policy lay in the enactment of the EU's General Data Protection Regulation (GDPR), the repeal of the Safe Harbour Agreement by the European Court of Justice, the Network Enforcement Act, the debate about a digital tax, proposals to dismantle digital platforms; the large fines imposed on US tech companies; and the involvement of China's Huawei company in the expansion of the 5G network in Germany.[22] A review of these differences shows that they occur in the following areas of digital policy:

- Safeguarding citizens' rights from state surveillance;
- Protecting the personal data of users of digital platforms;
- Taxation of new digital and above all data-based business models;
- Ensuring fair economic competition in the age of the platform economy.

There are some clear differences between European and US cyber security policies. However, they tend to be divergent approaches and differing priorities rather than extreme differences.[23]

**The differences in European and US cyber security policies mostly constitute divergent approaches and differing priorities.**

**How Extreme Are the Differences?**

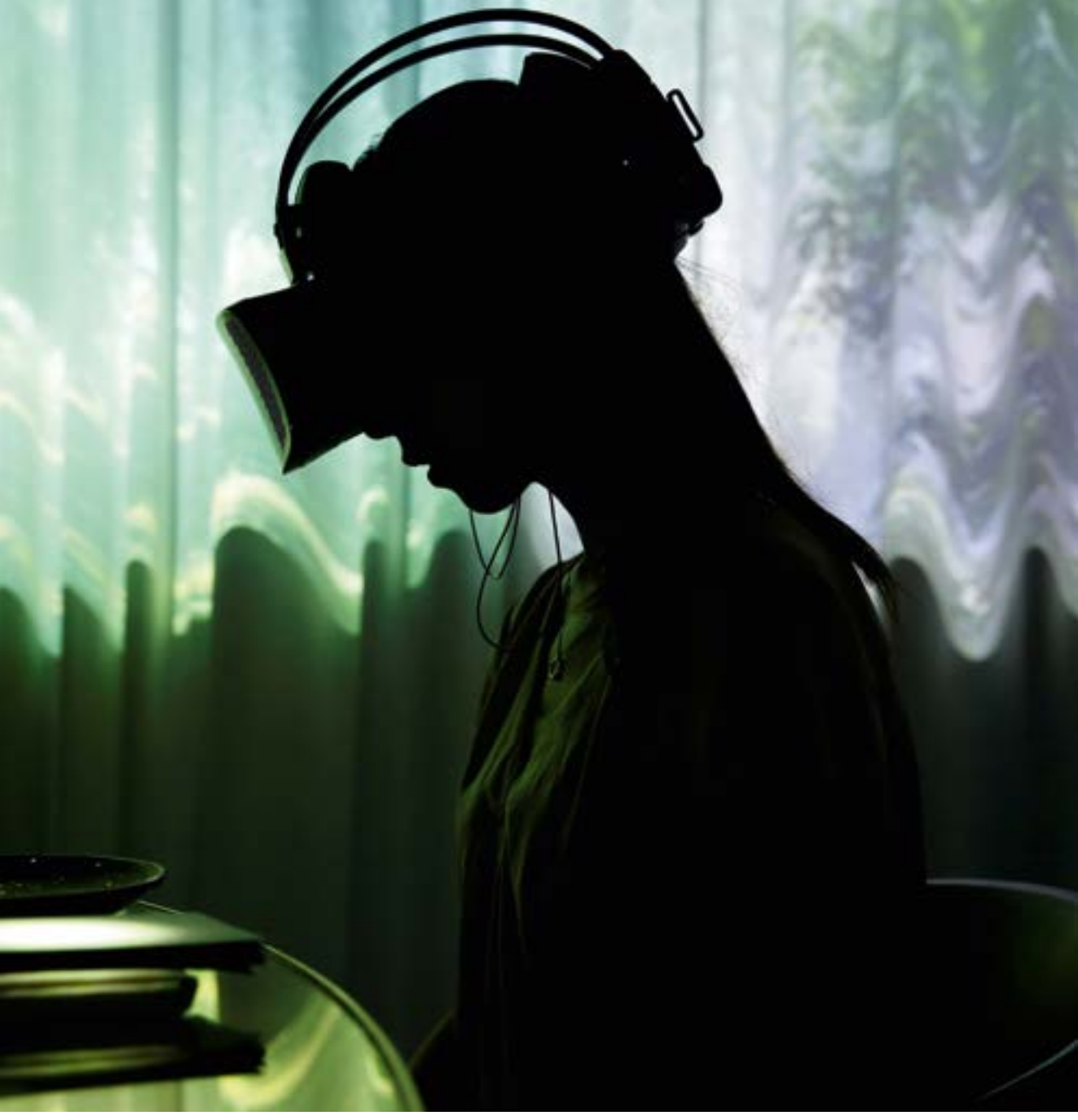
A Closer examination of the specific areas reveals that the current differences are not the result of fundamentally different worldviews and do not harbour any glaring conflicts of interest. The differences can be traced back to varying normative emphases, diverging regulatory approaches and different starting points for digital progress. Consequently, and in view of the need for transatlantic cooperation, these are differences that can and should be addressed within the framework of existing discussion forums on digital policy. With its more explorative and technology-friendly attitude, the US focuses on economic growth and national security interests and, under Donald Trump, is pursuing a more free-market approach regarding forms of co- and self-regulation as preferred to government regulation. Since most of the world's tech giants are US corporations, it is natural that, in terms of the economy and innovation, the US has a greater interest in protecting their economic freedom and associated role as major drivers of new technology. This is offset by a European approach that is more focused on protecting privacy, citizens' rights and the future viability of the European economy. To do this, it relies more strongly on legislation to regulate businesses, including mechanisms for imposing financial sanctions. Nevertheless, we should not fall into the trap of seeing these two approaches as being diametrically opposed. Of course, Europe also regards economic growth and the entrepreneurial freedom, which is needed to achieve this, as vital for ensuring the continuation of the digital revolution in the right direction. However, the continent is also aware of the need to find a balance between regulation and openness to innovation.[24] The fact that German, European and US interests overlap, despite some discrepancies in the area of digital security, is illustrated by the cooperation between European security authorities and the US intelligence services. The increasingly intense discussion about the role of China's Huawei Group in the development of the 5G network in Germany also shows that similar security risks are being identified on both sides of the Atlantic and that there is a close exchange of views on shared security risks.[25] Furthermore, a close examination of the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure of 2017 and the USA's latest National Cyber Strategy reveals that both these documents stress the importance of international cooperation in the field of cyber security and the need to continue working on an international normative framework.[26]

**In This Context, What Do We Need to Consider in the Coming Months and Years?**

With particular reference to calls for Europe to have more digital sovereignty, it is important to bear in mind that, despite all the differences that exist, the US is still a necessary and important partner that shares a very similar foundation of values with Europe, as opposed to China's model of digital authoritarianism. This implies that Germany and Europe, together with the US, should aim to advance digital innovation particularly in those areas where the need for transatlantic cooperation converges with shared interests. In light of the challenge to the political order posed by this digital authoritarianism, it is important to jointly address those risks that threaten the freedom, economic prosperity and political stability of the West.[27] However, over the coming months and years it must be borne in mind that a particularly high risk of conflict is associated with European regulations on digital policy that specifically target US tech giants, and it may collide with the US government's legitimate interest in protecting these companies. This does not mean that Europe should abandon its standards, but recognising this potential for conflict should lead to greater awareness of the need for dialogue and transparency. This should be accompanied by calls for an intensive transatlantic debate on how to shape the digital future.

**Where Is Rapprochement Already Occurring? Why Is Cooperation Not Just Necessary but Possible?**

A look into the recent past shows that, even in controversial areas, rapprochement is not just necessary, but possible. After the European Court of Justice's ruling on 6 November 2015 that the existing Safe Harbour Agreement was invalid, the US and EU managed to draft and ratify a new agreement in the space of just a few months. The new EU-US Privacy Shield Agreement came into force on 1 August 2016. This illustrates how it is possible to reconcile the different approaches to data protection in a relatively short period of time. A set of instruments was also created to harmonise the different jurisdictions in favour of the free flow of data but without the need to bring them completely into line. Even though the US and EU had very different ideas about data protection, the economic interests involved provided a strong incentive to quickly come to an agreement. Turning to the present, there are



Ubiquitous: The digital pervasion of our daily lives will continue to increase in the future.
Source: © Kim Kyung-Hoon, Reuters.

more signs that change is possible, even in the area of data protection. For example, it should be noted that, despite all the criticism of the EU's GDPR, more and more major US companies are now adopting the regulations for the whole of their global operations (e.g. Microsoft and IBM) or have announced their intention to do so (Facebook, Apple). At the state level, California has also enacted legislation similar to the GDPR. Of late, there have also been increasing signs that, as a result of several scandals surrounding Facebook and Europe's GDPR, the current US government is considering strengthening data protection at the national level.

It is also possible to perceive a shift in the West's relations with China regarding digital policy. This is because the US has been taking a much more confrontational line since Donald Trump took office, leading to fundamental changes to the Obama-era approach to US-China cyber diplomacy.[28] But Europe has also begun to take more decisive action against the outflow of strategically relevant key technologies and innovations, as well as against infringements of intellectual property rights.[29]

Internet governance is another field where cooperation is both possible and desirable. In this area, the US, Europe and other democratic partners have been resisting authoritarian efforts to create an alternative model for the virtual sphere for some years. The West and its partners uphold the liberal idea of a free and open internet in various formats.[30] While Europe currently aims at promoting the development of standards in cyber space,[31] the area of cyber diplomacy in general and internet governance in particular has been largely ignored in the US. Nevertheless, a closer look shows that the U.S. Department of State is still pursuing the Internet Freedom Agenda and the topic is also on the radar of the US Senate.[32] Major US companies have also become actively involved in this area over recent years because they see the dangers posed by increased fragmentation. Businesses could suffer if there is no harmonisation of standards in this respect.[33] A useful starting point in this area would be to continue pushing for closer ties between this issue and the area of cyber security, as there appears to be a window of opportunity for further developments under the current US administration.

**A Final Word of Caution**

When we look at how digital innovation is being shaped, it is clear that working with the US may not always be easy, but it is an important partner for Germany and Europe after all. If there is to be talk of Europe increasingly asserting itself against the US, then it is important to bear in mind their shared values and interests in the face of the resolve displayed by their authoritarian challengers. In Europe we should focus less on fixed regulatory boundaries with the US and look at more important issues, such as how the US was able to take on the role of digital pioneer, and what lessons Germany and Europe can and must draw from this in order to shape their own digital future.

*–translated from German–*

**Sebastian Weise** is Desk Officer for Global Innovation Policy at the Konrad-Adenauer-Stiftung.

1 Cf. i. a. Damen, Mario / Przetacznik, Jakub 2018: The European Union and its trade partners, European Parliament, Oct 2018, in: https://bit.ly/2txfn88 [20 Feb 2019]; cf. Hamilton, Daniel S. / Quinlan, Joseph P. 2018: The Transatlantic Economy 2018, Center for Transatlantic Relations, p. VII, in: https://bit.ly/2T6lNGD [21 Jan 2019]; Manyika, James / Lund, Susan / Bughin, Jacques / Woetzel, Jonathan / Stamenov, Kalin / Dhingra, Dhruv 2016: Digital globalization: The new era of global flows, McKinsey Global Institute, Feb 2016, in: https://mck.co/2k8ozxW [21 Jan 2019].

2 Cf. i. a. Metzler, Joshua P. 2014: The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment, Brookings Institute, 15 Oct 2014, in: https://brook.gs/2FMoFVi [21 Jan 2019]; cf. Mandel, Michael 2017: The Economic Impact of Data: Why Data Is Not Like Oil, Progressive Policy Institute, 12 July 2017, in: https://bit.ly/2sBwTYy [21 Jan 2019].

3 More specifically, the European Union is the destination of 45 per cent of all digitally derivable service exports from the US and the origin of 46 per cent of US imports in this area. 53 per cent of digital goods and services imported from the US are used in Europe to produce goods and services, which are then re-exported. Another element of the transatlantic digital economy is e-commerce. In Germany alone, 48 per cent of all digital shoppers purchase from US-based companies, while 49 per cent of US digital shoppers purchase from European companies. The fact that more than 4,000 US companies are currently registered under the US-EU Privacy Shield so that personal data can be transferred relatively easily from the EU to the US also underscores their close digital and economic ties. Cf. i. a. Hamilton / Quinlan 2018, n. 1, pp. 24–26; cf. Suominen, Kati 2017: Where the Money Is: The Transatlantic Digital Market, Center for Strategic & International Studies, 12 Oct 2017, in: https://bit.ly/2W9vxld [21 Jan 2019]; cf. U.S. Department of Commerce 2018: Privacy Shield List, status 6 Dec 2018, in: https://bit.ly/2b0Ijdq [14 Feb 2019].

4 Cf. Hamilton / Quinlan 2018, n. 1, p. 24.

5 Cf. ibid., p. 24 f.

6 The Big Four tech companies of Google (Alphabet), Apple, Amazon and Facebook deserve a particular mention here. User and revenue statistics on the Big Four are available here. For Facebook see: Statista 2018: Social media, in https://bit.ly/2MleaJP [21 Jan 2019]; for Google: Statista 2018: Google, in: https://bit.ly/2MoIxio [21 Jan 2019]; for Amazon: Statista 2018: Amazon, in: https://bit.ly/2HqaKa1 [21 Jan 2019]; for Apple: Statista 2018: Apple, in: https://bit.ly/2FF0FnO [21 Jan 2019].

7 For American companies – which also play a key role in the USA's innovation ecosystem – Europe is very important as both a market and a data pool.

8 Cf. i. a. International Monetary Fund 2018: China's Economic Outlook in Six Charts, 26 June 2018, in: https://bit.ly/2UTuSUu [21 Feb 2019].

9 Cf. Layne, Christopher 2018: The US-Chinese Power Shift and the end of the Pax Americana, in: International Affairs 94: 1, p. 95.

10 Important technologies for the future include artificial intelligence, quantum computing, autonomous systems, big data, genetic engineering, biotechnology and renewable energies. Cf. i. a. Fischer, Sophie-Charlotte 2018: Artificial Intelligence: China's High-Tech Ambitions, CSS Analyses in Security Policy 220, Feb 2018, in: https://bit.ly/2Ho1GCl [21 Jan 2019].

11 Cf. i. a. Beckley, Michael 2012: China´s Century? Why America's Edge Will Endure, International Security 36: 3, pp. 42–78.

12 While China walls off its national digital and technological market citing security interests (information security), it is actively involved in the Western digital economy, pressing ahead with the outward flow of key digital technologies and innovations. It also does not shy away from industrial espionage and intellectual property theft. Cf. Segal, Adam / Hoffmann, Samantha / Hanson, Fergus, Uren, Tom 2018: Hacking for ca$h: Is China still stealing Western IP, Australian Strategic Policy Institute; cf. Shalal, Andrea 2018: Germany risks losing key technology in Chinese takeovers – spy chief, Reuters, 11 Apr 2018, in: https://reut.rs/2Mni0Ci [21 Jan 2019].

13 Cf. i. a. Burgers, Tobias / Robinson, David R. S. 2018: Networked Authoritarianism is on the Rise, in: Sicherheit und Frieden 34: 4, pp. 248–252; cf. Mitchell, Anna / Diamond, Larry 2018: China's Surveillance State Should Scare Everyone, The Atlantic, 2 Feb 2018, in: https://bit.ly/2DZ0hMy [21 Jan 2019]; cf. The Economist 2018: China has turned Xinjiang into a police state like no other, The Economist, 31 May 2018, in: https://econ.st/2JkTBy5 [21 Jan 2019].

14 Cf. i. a. Wright, Nicholas 2018: How Artificial Intelligence Will Reshape the Global Order, Foreign Affairs, 10 July 2018, in: https://fam.ag/2uKfxtd [21 Jan 2019]; cf. Benaim, Daniel / Gilman, Hollie R. 2018: China's Aggressive Surveillance Technology Will Spread Beyond Its Borders, Slate, 9 Aug 2018, in: https://bit.ly/2Mu4Ouv [21 Jan 2019].

15 Cf. i. a. Weber, Valentin 2018: The Rise of China's Security-Industrial Complex, Blog Post Digital and Cyberspace Policy Program of the Council on Foreign Relations, 17 July 2018, in: https://on.cfr.org/2FF1Eo0 [21 Jan 2019]; cf. Romaniuk, Scott N. / Burgers, Tobias 2018: How China's AI Technology Exports Are Seeding Surveillance Societies Globally, The Diplomat, 18 Oct 2018, in: https://bit.ly/2TYOLIJ [14 Feb 2019].

16 Cf. i. a. Hohmann, Mirko / Benner, Thorsten 2018: Getting Free and Open Right: How European Internet Foreign Policy Can Compete in a Fragmented World, Global Public Policy Institute, pp. 10–17. For a specific view of Russia, see Nocetti, Julien 2015: Contest and conquest: Russia and global internet governance, in: International Affairs 91: 1, pp. 11–130; for China, see Sacks, Samm 2018: China's Emerging Cyber Governance System, CSIS, in: https://bit.ly/2RHwLG0 [21 Jan 2019]; Sacks, Samm 2018: Beijing Wants to Rewrite the Rules of the Internet, The Atlantic, 18 Jun 2018, in: https://bit.ly/2REXcfp [21 Jan 2019].

17 Cf. i. a. Clinton, Hillary 2010: Remarks on Internet Freedom, 21 Jan 2010, in: http://bit.ly/2MkqlXe [21 Jan 2019]; cf. Lynch, Marc 2010: The Internet Freedom Agenda, Foreign Policy, 22 Jan 2010, in: https://bit.ly/2WfFEFs [14 Feb 2019]; cf. European Commission 2013: Internet Freedom, 8 Mar 2013, in: https://bit.ly/2iIoLhN [14 Feb 2019].

18 For example, at the time of the Snowden revelations, Germany's former Minister of Transport and Digital Infrastructure, Alexander Dobrindt, argued that Germans and Europeans had to regain their basic digital sovereignty from the USA. Cf. Backhaus, Michael / Lambeck, Martin S. / Uhlenbroich, Burkhard 2013: Minister Dobrindt gibt die Richtung vor. „Wir brauchen das schnellste Internet der Welt", interview, Bild, 22 Dec 2013, in: https://bild.de/-33955848.html [14 Feb 2019]; Furthermore see basically Gueham, Farid 2017: Digital Sovereignity, Fonation pour l'innovation politique, p. 9, 13, in: https://bit.ly/2R2XiIG [21 Jan 2019].

19 Cf. i. a. Bendiek, Annegret / Berlich, Christoph / Metzger, Tobias 2015: The European Union's Digital Assertiveness, SWP Comment 43, Aug 2015, in: https://bit.ly/2E2lrKK [14 Feb 2019]; cf. Bitkom 2015: Digitale Souveränität: Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa, in: https://bit.ly/2T5yEsN [21 Jan 2019]; cf. Gueham 2017, ibid.; cf. Hackenbroich, Jonathan 2018: Reality Bytes: Europe's bid for digital sovereignty, ECFR, 17 Oct 2018 in: https://bit.ly/2J64nFV [14 Feb 2019].

20 Central building blocks here include a unified European digital internal market; the creation of a high-level ecosystem for European research, development and innovation; an increase in technical sovereignty to the point of creating a cyber-space infrastructure; an integrated European data sphere; independent European regulation of digital platforms; and fair taxation of data-based business models.

21 Cf. i. a. Internet Governance Forum 2018: IGF 2018 Speech by French President Emmanuel Macron, 2018, in: https://bit.ly/2U8pvzQ [21 Jan 2019]; cf. Hackenbroich 2018, n. 19.

22 Cf. i. a. Lewis, Patricia / Parakilas, Jacob / Schneider-Petsinger, Marianne / Smart, Christoph / Rathke, Jeffrey / Ruy, Donatienne 2018: The Future of the United States and Europe: An Irreplaceable Partnership, Chatham House, 11 Apr 2018, pp. 11–15.

23 Cf. i. a. U.S. Chamber of Commerce 2018: Transatlantic Cybersecurity Report: Forging a United Response to Universal Threats, in: https://uscham.com/2FNX99U [21 Jan 2019]; cf. Lewis et al., ibid., pp. 15–21, 25–26.

24 Cf. i. a. European Political Strategy Centre 2016: Towards an Innovation Principle Endorsed by Better Regulation, 30 Jun 2016, in: https://bit.ly/2nbBRci [21 Jan 2019]. See also statements made as part of the EU's Single Market Strategy: European Commission, Internal Market, Industry, Entrepreneurship and SMEs, Industry. Innovation, in: https://bit.ly/2Ik9a5I [21 Jan 2019].

25 Cf. i. a. Heide, Dana / Scheuer, Stephan 2019: Sorge um Datensicherheit – Berlin erwägt, Huawei beim Netzausbau auszusperren, Handelsblatt, 17 Jan 2019, in: https://bit.ly/2HhVc88 [21 Jan 2019]; cf. Böhm, Markus 2018: USA warnen vor Chinas Einfluss auf 5G-Netz, Spiegel Online, 29 Nov 2018, in: http://spon.de/afmZV [14 Feb 2019].

26 Cf. The White House 2017: Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 11 May 2017, in: https://bit.ly/2tg9vmu [21 Jan 2019]; cf. The White House 2018: National Cybersecurity Strategy, p. 20.

27 A useful source of potential partners is the Freedom Online Coalition, an alliance of 30 governments that have come together to advocate for a free and open internet. See Freedom Online Coalition, in: https://freedomonlinecoalition.com [14 Feb 2019].

28 Cf. i. a. Miles, Tom 2018: U.S. and China clash over 'technology transfer' at WTO, Reuters, 28 May 2018, in: https://reut.rs/2FG0KaZ [21 Jan 2019]; cf. Fidler, David P. 2018: U.S. Cyber Diplomacy Requires More than an Office, Council on Foreign Relations, 26 Jul 2017, in: https://on.cfr.org/2FG0SY1 [21 Jan 2019].

29 In 2018, for example, the EU, in agreement with the US, opened a case against China at the WTO for unfair practices in the outflow of technology; in 2018, as in the past, it made repeated and specific complaints about Chinese infringements of intellectual property rights; and at the end of 2018, on the initiative of France, Germany and Italy, it also drafted legislation on reviewing foreign direct investment, with a view to stemming the outflow of important digital key technologies and innovations to China.

30 For an initial overview of European and US commitments to the free and open internet and the central principles in various strategy documents see e. g. Morgus, Robert / Sherman, Justin 2018: The Idealized Internet vs. Internet Realities (Version 1.0), pp. 10–13.

31 In order to further develop the normative framework in cyberspace, Europe is actively engaging in this field, i.a. within the G7/G8, in the context of the GGE (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security), as well as in the "Paris Call for Trust and Stability", which Emmanuel Macron presented on this year's Internet Governance Forum, and with supporting the "Contract for the web" initiative.

32 Cf. Segal, Adam 2018: The Internet Freedom Agenda: Not Dead, but Not Exactly Thriving Either, Council on Foreign Relations Digital and Cyberspace Policy Program BlogPost, 21 May 2018, in: https://on.cfr.org/2ISw7QR [14 Feb 2019].

33 The fact that US companies are also active in this area can be seen in Microsoft's initiatives in the area of cyber security and in the fact that US companies have signed the Paris Call for Trust and Stability.