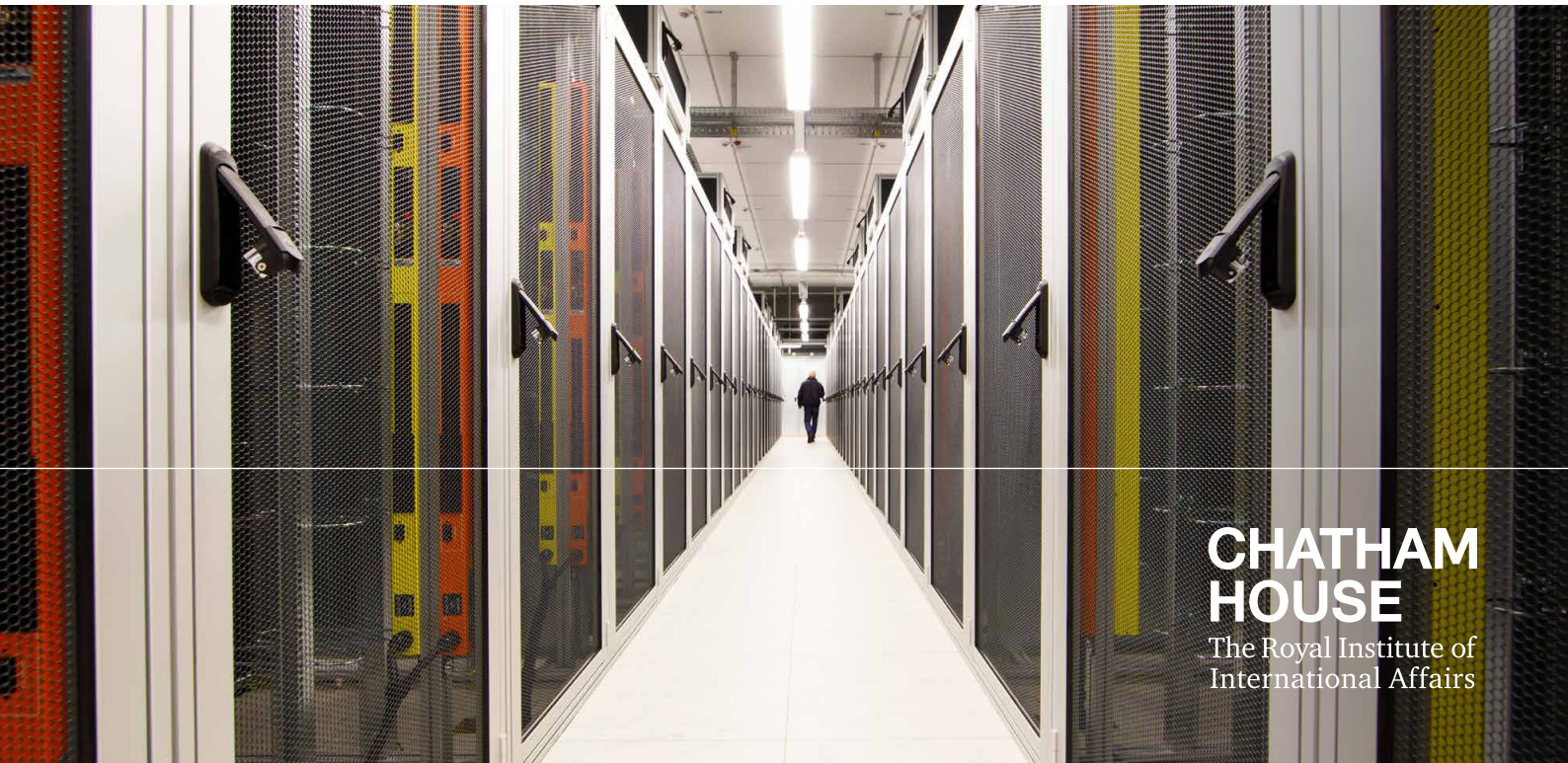
Research Paper

Christopher Smart
US and the Americas Programme | June 2017

Regulating the Data that Drive 21st-Century Economic Growth

The Looming Transatlantic Battle



CHATHAM HOUSE
The Royal Institute of International Affairs

Contents

Summary

- As the US government and European governments once again grapple with the challenges of reinforcing and expanding the transatlantic economic relationship, traditional negotiations over trade or tax policy may soon be upstaged by a far thornier and more important issue: how to regulate the storage, protection and analysis of data.
- Growth in the traditional global trade in goods and services has levelled off, but cross-border data flows continue to expand rapidly and the challenges of developing policies that protect privacy, security and innovation are already tremendous. For example, data analytics are driving dramatic productivity gains in industry, particularly for large and complex installations whose safety and efficiency will increasingly depend on flows of data across jurisdictions. Meanwhile, 'fintech' (financial technology) start-ups and large banks alike are testing new modes of accumulating, analysing and deploying customer data to provide less expensive services and manage the risk profile of their businesses.
- While the US debate on the use of data has often been framed around the trade-off between national security and personal privacy, Europeans often face an even more complex set of concerns that include worries that their digital and technology firms lag behind dominant US competitors. The political and regulatory uncertainty helps neither side, and leaves transatlantic companies struggling to comply with uncertain and conflicting rules in different jurisdictions.
- A global consensus on data regulation is currently well out of reach, but given the expanding importance of data in so many areas, basic agreement on regulatory principles is crucial between the US and the EU. This paper proposes a 'Transatlantic Charter for Data Security and Mobility', which could help shape a common understanding. While it would hardly resolve all concerns – or indeed contradictions – around the prevailing traditions on both sides of the Atlantic, it could provide the basis for better cooperation and establish a framework to protect the promise of the digital age amid an unpredictable and emotional debate.

1. Introduction

While trade and tax remain at the heart of the difficult economic conversations between Europe and the US, a new issue has emerged as a potential source of even greater friction: data. The rules that govern the collection, transmission and storage of data are perhaps one of the more surprising controversies in the transatlantic relationship. Similar liberal democracies with similar geostrategic interests might be expected to approach the handling of personal, corporate and government data in more or less the same way. And yet the US and its key European partners have struck different balances in the trade-offs between national security and citizens' rights, between freedom of expression and personal privacy, and between free enterprise and market regulation.

Embarrassing leaks, careful denials and endless lawsuits will continue to shape the awkward efforts of policymakers to find common ground around issues like cyberespionage, defence of common networks and the sharing of personal data with law enforcement. Cyberattacks with the aim of disrupting government operations or influencing election campaigns will add still further pressures.[1] These will all serve as a noisy backdrop to a related but separate debate over how commercial firms should exploit the opportunities of global networks and 'big data' analytics while protecting national interests and privacy. Setting common guidelines for commercial data transmission and storage remains crucial both to protect the goods and services that already depend on sophisticated data-gathering and analysis, and to support the next generation of productivity gains and business opportunities.

The productivity debate remains complicated, but there is little doubt that global firms yearn for clarity and predictability as they organize themselves to make the most of the data revolution. Neither is likely to become a reality soon. The EU's new General Data Protection Regulation (GDPR) will take effect in 2018, but its implementation will inevitably be coloured by the fact that American firms currently dominate the information technology business. Last year's 'Privacy Shield' agreement between the US and the EU renews the permission for firms with transatlantic business interests to transfer data, subject to compliance with basic standards of protection, but the agreement remains vulnerable to European court challenges. Britain's decision to leave the EU adds a further complication, as it establishes its own set of data protection rules that may not easily align with either European or US requirements. Meanwhile, the World Trade Organization (WTO) continues to debate new rules for digital trade, even as markets like China, Russia and Brazil make up their own. This makes more determined efforts by US and European policymakers to agree basic principles that will guide the usage and protection of personal and commercial data all the more important. While common regulations or even greater alignment among regulators seem out of reach, a 'Transatlantic Charter for Data Security and Mobility' would provide a set of principles for more specific rules amid political landscapes and technological developments that are evolving rapidly.

[1] The potential risks are certainly chilling. See, for example, Baylon, C., Brunt, R. and Livingstone, D. (2015), *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, Chatham House Report, London: Royal Institute of International Affairs, www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf; Livingstone, D. and Lewis, P. (2016), *Space, The Final Frontier for Cybersecurity?*, Research Paper, London: Royal Institute of International Affairs, www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

This paper examines how governments on both sides of the Atlantic are establishing frameworks that attempt to govern the commercial uses of data. Section 2 explores the promise of data analytics in driving new productivity growth across the economy, with particular focus on industry and finance where the changes are transformational. The 'industrial internet of things' will expand the data flows to manage everything from aircraft engines to gas pipelines, while the largest banks and insurers are responding urgently to the challenge from nimble start-ups with smarter analytics. Sections 3 and 4 of this paper review the policy context and political forces shaping data rules in the US and Europe respectively. Each jurisdiction takes the issue seriously, but each has inevitably developed responses that grow from a particular history, culture and political context. The final two sections propose a framework for US–European cooperation, including principles to guide choices on regulations and laws as well as recommendations for better institutional cooperation as policymakers struggle with emotional political forces, dynamic technological developments and the pressures to support productivity and economic growth. If this 'Transatlantic Charter for Data Security and Mobility' were adopted bilaterally, say as part of the annual reviews of the US–EU Privacy Shield agreement, it could form the basis for broader cooperation on these issues, helping to drive progress in the G7 and G20 and ultimately perhaps in trade agreements under the WTO.

2. Setting Rules for the Digital Economy

The challenges of setting data rules have grown with the quantity of data produced and the sophistication of data uses. Governments face both promise and peril. The promise lies in rapid improvements in economic productivity and in better tools to understand the needs of citizens or improve the quality of public services. The peril lies in the accumulation and analysis of data in ways that threaten privacy, civil rights or market competition.[2] Balancing these will involve recognizing that personal data, commercial data and industrial data raise different concerns and require tailored sets of rules. It will require a greater technological sophistication to resist, for example, apparently simple solutions like requiring that data remain localized in a single jurisdiction when cloud storage is likely safer and more efficient.[3] Finally, it will mean considered regulation that proscribes the anti-competitive practices of technological giants. Some of the most intriguing challenges lie in those parts of the economy – such as industry and financial services – where the use of data is upending traditional business models most quickly.

Data growth

Much of the commentary over the promise of the digital economy seems breathless – potentially exaggerating its impact – but the revolutionary transformation in some sectors is already undeniable and the risks are high for firms that are not thinking hard about the implications of the change. One report estimates that the digital universe will grow nearly 20 times during 2015–25 to 180 zettabytes (or 180 x 10^{21} bytes – 180 trillion gigabytes). To put this number in perspective, a single zettabyte could store the equivalent of 2 billion years of music or Tolstoy's *War and Peace* 323 trillion times.[4] Much of this growth will simply come from the ways in which documents, images and videos are increasingly stored digitally, but the pace will likely accelerate due to two additional forces. First, digital activity will catch up in emerging markets like China, India and Brazil, where records, analysis and commercial efficiencies have lagged. By one reckoning, these countries may move from contributing roughly one-third of the world's digital data to about two-thirds (with some 20 per cent in China alone).[5] Second, a new boost will come from the much-anticipated 'internet of things', which continues to expand with the falling cost of sensors and digital identification tags, the integration of connective networks and the sophistication of data analytics. Mobile broadband subscriptions now exceed one for every person on earth. Meanwhile, half of the vast and expanding trove of digital data

[2] The Obama administration addressed these issues in two reports that highlight some of the trade-offs. Even as it sought to make available vast government data sets on everything from the weather to student loans, it tightened restrictions on the government's use and storage of personal data. See The White House (2015), *Big Data: Seizing Opportunities, Preserving Values,* Executive Office of the President, https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; The White House (2016), *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, Executive Office of the President, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

[3] Increasingly, business leaders suspect that some of the most important regulators do not understand the full potential of big data analytics, and worry that uncoordinated and reactive approaches to privacy protection or national security concerns will constrict growth. See a fascinating set of interviews in Schroeder, R. (2016), 'Big data business models: Challenges and opportunities', *Cogent Social Sciences*, p. 13, 2: 1166924 http://dx.doi.org/10.1080/23311886.2016.1166924.

[4] IDC estimates cited in *The Economist* (2017), 'Data is giving rise to a new economy', 6 May 2017, www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy; Daily Infographic (2013), '2016: The Year of the Zettabyte', 23 March 2013, www.dailyinfographic.com/2016-the-year-of-the-zettabyte-infographic.

[5] Gantz, J. and Reinsel, D. (2013), *The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East – United States*, IDC View, www.emc.com/collateral/analyst-reports/idc-digital-universe-united-states.pdf.

has an IP address, which means the data can be accessed, compared, sorted and analysed at almost no cost.[6] The likely result will be not just the proliferation of data, but the exponential expansion of data uses – creating new avenues for business creation, service delivery and productivity growth in areas previously considered outside the once-segregated 'digital economy'.

More dramatically, perhaps, the flows of data across borders continue unabated and uncorrelated with trade growth. Global trade in goods and services has expanded more slowly since the 2008–09 financial crisis, and cross-border financial loans and investments have fallen as well.[7] But cross-border bandwidth usage has soared 45 times since 2005, and may grow another nine times over the next five years amid a continuing surge in digital commerce, video and cross-border storage.[8] These flows are driven by the falling costs of maintaining digital platforms, the swelling trade in purely digital goods (movies, music and media) and the proliferation of 'digital wrappers', the software that manages the operation of physical machines and goods often at a great distance and from a different jurisdiction. The impact is potentially significant for sectors ranging from shipping and energy to agriculture and healthcare – and almost everything in between.[9] In time, advances in artificial intelligence will expand the gains further still.[10]

The industrial internet

The popular press around the internet of things tends to focus on innovations with direct connections to consumers: refrigerators that report sour milk and mattresses that monitor sleep habits. Arguably, however, far greater impact on global economic productivity awaits with the deployment of the industrial internet of things, which can help monitor the operations of complex installations of capital equipment, enhance their efficiency and assess their maintenance needs much more precisely. While industrial firms have long been automating the ways in which they monitor installed systems, the ability to place more sensors and analyse the data they send in real time opens up broad new possibilities in automatic operational adjustments. Cheaper storage and processing, for example, allow the accumulation of detailed historical data across an industrial operation that can provide essentially 'predictive' recommendations for current maintenance and future efficiency.[11] Soon enough, the industrial internet will no longer be on the cutting edge of industrial innovation but the driving force of most industry (see Box 1).

Regulating industrial data

There are at least two large political headaches looming over the data revolution in industry. First, of course, governments and societies will have to scramble to find new ways to support job creation at a speed that compensates for the losses from automation and technology. This

[6] Evans, P. and Forth, P. (2015), 'Borges' Map: Navigating A World of Digital Disruption', Boston Consulting Group, pp. 8–9.
[7] World Trade Organization (2016), *World Trade Statistical Review 2016*, www.wto.org/english/res_e/statis_e/wts2016_e/wts2016_e.pdf.
[8] Manyika, J., Lund, S., Bughin, J., Woetzel, J., Stamenov, K. and Dhingra, D. (2016), *Digital globalization: The new era of global flows*, McKinsey Global Institute, pp. 30–37, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.
[9] DuBravac, S. and Ratti, C. (2015), *The Internet of Things: Evolution or Revolution?*, AIG and Consumer Electronics Association, December 2015, pp. 9–14, www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/aig-white-paper-iot-june2015-brochure.pdf.
[10] Henke, N., Bughin, J., Chui, M., Manyika, J., Saleh, T., Wiseman, B. and Sethupathy, G. (2016), *The age of analytics: Competing in a data-driven world*, McKinsey Global Institute, pp. 6–8, www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world.
[11] Patel, S. (2016), *Unlocking Business Value Through Industrial Data Management*, GE Digital, www.ge-ip.sk/media/gedis/cmsfiles/files/Unlocking%20Business%20-%20Industry%20data%20management.pdf. See also Winoker, S. E. and Moerdler, M. L. (2016), *Industrial Internet: The Digital Dream – A Primer, and What It Really Means for the Future of Industrial and Software Stocks*, Sanford C. Bernstein LLC.

is not a new problem, but the speed of job losses may soon increase sharply. Optimists argue that the transformation boosts productivity, which should raise consumer incomes and drive economic growth as it frees workers for as yet uncontemplated jobs that add more value to the economy. They view growth as not only inevitable but desirable, especially at a moment when developed markets are consumed by debates over 'secular stagnation'. The pessimists see it as the classic destruction of jobs, with little or nothing on the horizon to offer a replacement for low-skilled workers. They see this as fuel for populism in wealthier countries, where income inequality is rising, and an outright disaster in developing countries, where low-wage workers have offered a comparative advantage in traditional manufacturing and a path out of poverty.[12]

This important debate is beyond the scope of this study, but the political forces that align on either side will also shape the discussions around the second looming political headache: the appropriate handling of industrial data.[13] Few jurisdictions have come to terms with the complexities of these issues. In a political environment that is increasingly focused on the vulnerability of personal data, the protection and management of industrial data will inevitably turn emotional very quickly even if the industrial applications themselves do not mainly raise issues of personal privacy. Large aggregations of such data that must be gathered and compared seamlessly across borders will quickly raise national security concerns, especially where they touch critical infrastructure. When breaches of personal databases have already triggered knee-jerk calls for data localization in Brazil and tightly regulated data access in Europe, ill-considered rules could quickly undermine the promise of the industrial internet. China, Russia and Iceland have all adopted various forms of data localization requirement, creating a patchwork of self-defeating and sometimes contradictory regulations that firms must navigate.[14] By one estimate, rules restricting data flows just among member states of the EU cost its citizens $193 billion per year.[15]

> Large aggregations of data that must be gathered and compared seamlessly across borders will quickly raise national security concerns, especially where they touch critical infrastructure. When breaches of personal databases have already triggered knee-jerk calls for data localization in Brazil and tightly regulated data access in Europe, ill-considered rules could quickly undermine the promise of the industrial internet.

Manufacturers may be able to mitigate some of these challenges in early conversations with political leaders and regulators, who may not yet fully appreciate the need to balance security and privacy concerns with the promise of tremendous gains in productivity and growth. Governments may also not fully understand the potential benefits of industrial internet analytics to their own roles as

[12] Prominent among the optimists are Brynjolfsson, E. and McAfee, A. (2014), *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies,* New York: W. W. Norton & Company. A more pessimistic conclusion comes from Gordon, R. (2016), *The Rise and Fall of American Growth: The U.S. Standard of Living Since the Civil War*, Princeton, NJ: Princeton University Press. The problem for developing countries has been outlined by Rodrik, D. (2016), 'Premature De-Industrialization', *Journal of Economic Growth*, 21: 1–33. Jason Furman, former chairman of President Obama's Council of Economic Advisers, offers a thoughtfully even-handed approach in Furman, J. (2016), 'How to Protect Workers from Job-Stealing Robots', *The Atlantic*, 21 September 2016, www.theatlantic.com/business/archive/2016/09/jason-furman-ai/499682/.

[13] Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J. and Aharon, D. (2015), *The Internet of Things: Mapping the Value Beyond the Hype*, McKinsey Global Institute, p. 114, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[14] Ahmed, M. (2015), 'Complexity of data rules weaves a tangled web', *Financial Times*, 20 May 2015, www.ft.com/content/baf074da-cc8e-11e4-b5a5-00144feab7de.

[15] Bauer, M., Ferracane, M. F., Lee-Makiyama, H. and van der Marel, E. (2016), 'Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States', European Centre for International Political Economy Policy Brief, No. 3, http://ecipe.org/publications/unleashing-internal-data-flows-in-the-eu/.

regulators.[16] The same data and analytics that improve the efficiency of a power plant or an aircraft engine, for example, can help government officials better monitor safety and emissions. Ultimately, this new transparency on industrial operations can also help set more precise efficiency targets in regulated industries. Because the number of industrial installations is relatively small in any one country, however, the analysis will only be reliable if data can be compared meaningfully across borders. This will likely be an acrimonious debate, but manufacturers have a strong case for rules that secure the long-term benefits of these new industrial configurations.

Box 1: The industrial internet of things

Estimates of the potential size of the industrial internet vary widely. One survey projects that the number of connected 'things' will rise by 31 per cent in 2017 over the previous year.[17] Another predicts that by 2025 there will be more than 150,000 new devices connected to the internet every minute.[18] Some projections go so far as to estimate that the industrial internet will far outstrip the value of the consumer internet by 2025, delivering as much as $8.6 trillion in additional annual value.[19] A more concrete and immediate measure of the promise can be found in the $2.2 billion that flowed into venture capital investment in 2016 for technologies that track supply chain movement, manage vehicle fleets or provide bespoke cloud and security solutions for industrial clients.[20] This marked the sixth straight year of growth. By some estimates demand for industrial software has grown faster in the heavy industry, automotive and healthcare sectors than in any others.[21] Major players in both hardware and software are already endeavouring to establish common standards that promote interoperability, enhance data security and accelerate the growth of the industrial internet.[22]

The variety of applications is striking:

- Shell Oil has been testing new sensors on its exploration and production equipment, gathering temperature, pressure and other readings from compressors, generators and drills to improve operational efficiency and reduce maintenance costs. Advanced algorithms specify parts that need maintenance or repair.[23]
- Rockwell Automation has produced systems that integrate sensors in trucks at fracking operations and unmanned liquefied natural gas (LNG) distribution facilities to boost operational efficiency.[24]
- German airline Lufthansa has launched a platform that combines monitoring of conditions across operations with analytical tools that predict precisely when aircraft components should be replaced and recommend measures that can enhance safety, improve fuel consumption and optimize the use of expendable parts.[25]

[16] In fact, the US Federal Trade Commission issued a report arguing that 'any Internet of Things-specific legislation would be premature at this point in time given the rapidly evolving nature of the technology'. See Federal Trade Commission (2015), 'FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks', 27 January 2015, www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices. The National Telecommunications and Information Administration (NTIA) has been working with industry as well to outline a framework for potential regulations and standards.
[17] Gartner (2017), 'Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016', press release, 7 February 2017, www.gartner.com/newsroom/id/3598917.
[18] Press, G. (2016), 'IoT Mid-Year Research Update from IDC and Other Research Firms', *Forbes*, 5 August 2016, www.forbes.com/sites/gilpress/2016/08/05/iot-mid-year-update-from-idc-and-other-research-firms/#4c10a5d255c5.
[19] Annunziata, M. (2015), *The Moment for Industry*, General Electric, October 2015, www.ge.com/digital/sites/default/files/Annunziata_Moment-for-industry.pdf.
[20] CB Insights (2017), 'Industrial IoT Hits Another Annual High in Deals and Dollars', 10 March 2017, www.cbinsights.com/blog/industrial-iot-startup-funding/.
[21] Gartner estimates, cited in Troman, M., Virgo, A., Obin, A., King, J., Kaloghiros, M. and Elster, J. (2016), 'Global Primer: Digital Machinations', Merrill Lynch, 9 September 2016, p. 15.
[22] Alessi, C. (2017), 'GE, Siemens Vie to Reinvent Manufacturing by Harnessing the Cloud', *Wall Street Journal*, 5 March 2017, www.wsj.com/articles/ge-siemens-vie-to-reinvent-manufacturing-by-harnessing-the-cloud-1488722402. A global consortium including AT&T, Cisco, General Electric, IBM and Intel established the Industrial Internet Consortium (IIC) in 2014. Hardy, Q. (2014), 'Consortium Wants Standards for 'Internet of Things'', *New York Times*, 27 March 2014, https://bits.blogs.nytimes.com/2014/03/27/consortium-wants-standards-for-internet-of-things/?_r=0.
[23] Troman et al. (2016), 'Digital Machinations', Merrill Lynch, p. 39.
[24] Winoker and Moerdler (2016), *Industrial Internet*, p. 5.
[25] Van Wagenen, J. (2016), 'Lufthansa Launches Predictive Maintenance Platform', *Aviation Today*, 19 October 2016, www.aviationtoday.com/2016/10/19/lufthansa-launches-predictive-maintenance-platform/.

- Dundee Precious Metals, a Canadian mining company, worked with Cisco to deploy wireless access points in mining tunnels and attached digital tags to both employees and equipment to better manage their activities. The results pushed the mine's utilization rate close to 100 per cent while tripling production.[26]
- Bharat Light and Power, one of India's largest clean energy companies, now draws analytics from IBM software to improve the efficiency of its remote wind farms and predict servicing needs.[27]

Even firms that have begun to develop an industrial internet strategy are far from exploiting its full benefits.[28] For example, on average only 1 per cent of the data collected on an oil rig with 30,000 sensors are currently examined. Even that sampling is mainly analysed to detect operational anomalies rather than improve efficiency or foresee problems.[29] As automated systems and robots become ubiquitous, software and data analytics will become an ever more important element in what has traditionally been entirely an activity of physical production.[30]

Data revolution and financial services

If the promise of data analytics puts the industrial sector on the verge of massive transformation, it may not be an exaggeration to describe the changes under way in financial services as revolutionary. Whether in banking, insurance or investment, financial activity involves gathering and analysing data better, faster and cheaper than competitors in order to properly assess and price risks. The data revolution now offers significantly more effective tools to do just that. Traditional banks and insurance companies have been struggling with the possibilities and pitfalls brought about by the oceans of data as they try to better track clients, loans and investments.

The five largest US banks, for example, control about half of the industry's assets. Through economic cycles and financial crises, most of these firms have found strength in their size. When it comes to managing data, however, size is not necessarily an advantage given how they grew. Sometimes they grew organically. Sometimes it was through strategic acquisition. Often, strong banks were encouraged to take over weaker institutions. As a result, the overwhelming preponderance of financial services are delivered from a hodgepodge of computer systems cobbled together for almost any reason other than to provide better gathering and analysis capabilities. Such banks not only rely on legacy systems that may be vulnerable to failure, their very business models make easy targets for newer and more nimble start-ups that can offer clients better service for less.[31] At least one measure of the promise – and the threat – from these start-ups is the $5 billion of venture capital that has flowed annually into new 'fintech' firms.[32]

[26] Troman et al. (2016), 'Digital Machinations', p. 39.
[27] *Express Computer* (2014), 'IBM Gives BLP a Clean Edge', 16–31 January 2014, pp. 26–28, https://issuu.com/indianexpressgroup/docs/jan_16-31_express_computer-01-52; Pearson, N. O. (2013), 'Bharat Light and Power Partners with IBM to Boost Wind Farm Output', Bloomberg, 19 November 2013.
[28] Only 8 per cent of firms studied by Verizon/Oxford Economics are using more than a quarter of the data they generate. Cited in Troman et al. (2016), 'Digital Machinations', Merrill Lynch, p. 42. See also Henke et al. (2016), *The age of analytics*, pp. 29–41.
[29] Manyika et al. (2015), *The Internet of Things*, p. 4.
[30] Global robot installations are rising at roughly 15 per cent annually according to the International Federation of Robotics. The economic impact of robots could reach up to $1.2 trillion by 2025, according to McKinsey. Both cited in Troman et al. (2016), 'Digital Machinations', p. 53.
[31] Jo Ann Barefoot, a former senior US regulator and thoughtful author on financial and regulatory technology, cites five trends that are driving much of the transformation: big data, artificial intelligence, voice technology, digital currency and blockchain, and online and mobile technologies. See Barefoot, J. A.(2016), 'Regulation Innovation/Briefing 1: The Five Tech Trends', 11 May 2016, www.jsbarefoot.com/blog/2016/5/11/second-teaser-to-my-new-video-series-the-five-tech-trends.
[32] See KPMG and CB Insights (2016), 'The Pulse of Fintech, Q3 2016', https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/11/the-pulse-of-fintech-q3-report.pdf. Also Belinki, M., Rennick, E. and Veitch, A. (2015), 'The Fintech 2.0 Paper: Rebooting Financial Services', Santander Innoventures, Oliver Wyman and Anthemis Group, http://santanderinnoventures.com/fintech2/. For an overview of the opportunity for the financial services sector from the perspective of a software firm, see Oracle (2015), *Big Data in Financial Services and Banking: Architect's Guide and Reference Architecture Introduction*, Oracle Enterprise Architecture White Paper, www.oracle.com/us/technologies/big-data/big-data-in-financial-services-wp-2415760.pdf.

Regulating financial data

For governments and regulators, these data flows offer the prospect of greater transparency in financial activity than ever before. Bank balance sheets and loans can be monitored.[33] Insurance risk can be tracked. Underlying collateral can be evaluated. The increasing role that banks and other financial institutions play in tracking down criminals and terrorist groups can only be enhanced with the proper handling and analysis of the data.[34] This, at least, is the potential vision, notwithstanding enormous legal, institutional, accounting and political barriers. On the other hand, the challenges seem far more daunting. Above all, the expanding flows of financial information sharpen questions around personal privacy, as financial firms find new ways to analyse and aggregate it for their own business development. There are also risks of cyberattacks that steal consumer data or that disrupt and disable the key infrastructure that underpins global financial markets.

The increasing role that banks and other financial institutions play in tracking down criminals and terrorist groups can only be enhanced with the proper handling and analysis of the data.

Regulators struggling to keep up have explored experimental models of regulating these dynamic start-ups. The UK's Financial Conduct Authority has established a so-called 'sandbox' in which new financial technology business models can operate on a small scale as regulators monitor their activities. US policymakers are debating similar approaches.[35] On a separate front, battle lines are drawn between the Davids and Goliaths of financial services over requirements that traditional banks allow the sharing of account information in digital form should a customer wish to use the services of a financial planning start-up or another investment manager. Traditional banks insist their main concern is the security of client data, while the threat to their operating model is also clear.[36] The long-term challenge will be to process such data, while protecting the confidentiality of clients, satisfying the national security concerns of governments and defending against cyberattacks. These will become important questions for US and European regulators, as they scramble to keep up with the most complex and dynamic financial and technological firms handling the world's largest data flows.

[33] The European Central Bank has undertaken a particularly ambitious effort to gather granular data on loans through national central banks. The AnaCredit (for analytical credit datasets) Regulation came into effect in November 2016 and actual data collection will start in 2018. See European Central Bank (2016), 'AnaCredit', www.ecb.europa.eu/stats/money_credit_banking/anacredit/html/index.en.html.
[34] Zarate, J. (2013), *Treasury's War: Unleashing a New Era of Financial Warfare*, New York: Public Affairs.
[35] Roughly, firms must demonstrate that they have enough resources to compensate customers who may be harmed, but regulators agree to withhold any fines or penalties while these start-ups experiment with new business models. See Financial Conduct Authority (2015), 'Regulatory Sandbox', www.fca.org.uk/publication/research/regulatory-sandbox.pdf; Witkwoski, R. (2016), 'U.S. House Bill Aims to Set Up 'Sandbox' for Fintech Innovation', *Wall Street Journal*, 22 September 2016, www.wsj.com/articles/u-s-house-bill-aims-to-set-up-sandbox-for-fintech-innovation-1474539893.
[36] In Europe, lines have been drawn around the implementation of the second Payment Services Directive, so-called PSD-2, approved in November 2015. In the US, the battle is over the implementation of Section 1033 of the Dodd-Frank Act. See Demos, T. (2017), 'Fintech Startups Want to Save One Key Page of Dodd-Frank', *Wall Street Journal*, 2 February 2017, www.wsj.com/articles/fintech-startups-want-to-save-one-key-page-of-dodd-frank-1486035001.

Box 2: The data revolution in financial services

In financial services, what is perhaps most remarkable is just how directly the data revolution helps predict risks more accurately, engages clients more efficiently and thus presents enormous competitive pressures to traditional business models. Some specific commercial applications are as follows:

- The insurance industry, which now has relatively indirect contact with clients through independent brokers, can keep much better tabs on the risks it is actually underwriting. Distributed sensors can better monitor home security, personal health and safe driving habits, potentially reducing both payouts and premiums – even as the proliferation of such technology raises a tangle of privacy concerns. (Italy's Octo offers technology that monitors driver's habits, including how fast they accelerate and brake, collecting driving data on 60,000 miles driven every minute.) Firms can then charge premiums, up to 30 per cent less, based on a more precise measure of driving risk.[37]
- Leasing companies – with some help from the industrial internet – can better monitor the condition of equipment, offering rebates to good clients or imposing penalties for misuse. They can also calculate residual value in real time for a more accurate view of their own balance sheets.[38]
- Blockchain technology and self-executing distributed ledger contracts promise to reduce the costs of trade finance significantly. Changes to one copy of the ledger are automatically and instantly updated across all the rest, which eliminates the need for a third-party intermediary in a contract.[39] Embedded sensors on traded goods feed real-time information to update electronic bills of lading. Sellers, buyers and banks will have accurate information on the location and condition of cargo, and payment can be triggered automatically upon proper delivery.[40]
- Banks can better track and value the collateral they hold against their loan books, as sensors provide an update on its condition and eliminate the need for costly on-site inspections. Conceivably, they can also directly monitor the financial condition of their borrowers with regular data on inventory levels, pricing pressures and sales bookings.[41]

Meanwhile, as the industrial internet begins to deliver gains in productivity and savings to the operators of turbines, rigs and pipelines, there likely remain significant untapped opportunities in finance as well. The networks of sensors and big data analytics that help prescribe more efficient maintenance schedules and predict potential system failures can also deliver new levels of transparency to those who provide loans and insurance to these industrial and infrastructure investments. Especially in developing countries, where operational and political risks are already high, analytics that can monitor operations and productivity gains should help attract new pools of money from otherwise skittish financiers.[42] Initially, fully realizing these benefits will require the design of aggregated data streams that genuinely predict outcomes based on other similar operations and demonstrably reduce risk.

[37] International Institute of Finance (2016), *Innovation in Insurance: How Technology is Changing the Industry*, p. 9, www.iif.com/system/files/32370132_insurance_innovation_report_2016.pdf. In the US, Progressive Insurance developed a similar product called Snapshot.
[38] Eckenrode, J. (2015), *The derivative effect: How financial services can make IoT technology pay off*, Deloitte University Press, 2015, p. 14, https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-financial-services-industry.html.
[39] See this slightly sceptical primer by Iansiti, M. and Lakhani, K. R. (2017), 'The Truth about Blockchain', *Harvard Business Review*, January–February 2017, https://hbr.org/2017/01/the-truth-about-blockchain. However, raised eyebrows have not deterred the Depository Trust and Clearing Corporation (DTCC), a global repository for credit derivative transactions, from announcing plans to move its database to blockchain. Murphy, H. (2017), 'Database move gives blockchain its first test case', *Financial Times*, 9 January 2017, www.ft.com/content/aeb63b96-d64b-11e6-944b-e7eb37a6aa8e.
[40] Belinki, Rennick and Veitch (2015), 'The Fintech 2.0 Paper', pp. 8–9.
[41] Inefficiencies in the global collateral management market are estimated to cost banks up to $4 billion annually. Cited in Belinki, Rennick and Veitch (2015), 'The Fintech 2.0 Paper', p. 11. Also, Alibaba's finance outfit has used data on real-time merchant transactions to create an internal credit rating system that generates better non-performing loan ratios than traditional banks. Henke et al. (2016), *The age of analytics*, p. 27.
[42] New regulatory regimes likely overstate the risk of infrastructure assets. Despite their low-risk nature, Basel III and Solvency II require high-risk capital allocations for infrastructure investments. However, providing real-time data and clarity on the operations of machinery may help regulators to better understand the risks, better predict the cashflows and better support these crucial investments for the economy.

3. US Approaches to Data Regulation

The debate in the US over data policy has largely been shaped by traditional concerns about privacy and national security, even if firms have long sought to influence specific rules that affect their own profits.[43] In recent years, and especially since the 2013 public revelations of intelligence contractor Edward Snowden, the conversation now embraces a dawning awareness of both the risks of growing dependence on data analytics and their crucial importance to future productivity.

Privacy and US law

While there is, in fact, no specific fundamental right to privacy in the US constitution, the jurisprudence around privacy laws in the US is extensive and well developed. A substantial patchwork of laws and court decisions have set forth protections for personal information, including the 1970 Fair Credit Reporting Act, which regulates the handling of credit data, and the 1974 Privacy Act, which regulates government collection of personal information.[44] Over time, many state and local governments have also introduced data breach notification laws requiring the disclosure of breaches in databases containing personal information.[45] Even if law and practice still seem to lag behind the potential of technology and commerce, regulators and lawmakers have worked hard to strike the right balance between personal privacy and national security.

Data interception

The Barack Obama administration engaged these debates most prominently through three highly charged political issues. First, and perhaps least dramatic, were efforts to reform and update the 1986 Electronic Communications Privacy Act (ECPA), which set guidelines for law enforcement monitoring of early electronic communications long before the advent of the cloud or most remote computing services. Congress has held lengthy hearings on the issues, but the debate continues to intensify around matters of law enforcement, access to cloud storage and whether the data owner must be notified as an investigation unfolds.[46] While the House of Representatives passed an update in 2016, the Senate has yet to act and the Trump administration has yet to state a view. In a separate, but related matter, a US federal court ruled in July 2016 that the US government cannot seize data from foreign data centres under the Stored Communications Act. This protected Microsoft from a lower court order to turn over the contents of an email account stored in Ireland, but opened many new challenges for governments about how to secure access to data under legitimate law enforcement

[43] Under pressure from industry, for example, in early 2017 Congress repealed privacy rules for broadband providers deemed cumbersome by telecommunications and cable firms. Byers, A. (2017), 'House votes to revoke broadband privacy rules', Politico, 28 March 2017, www.politico.com/story/2017/03/house-votes-to-revoke-broadband-privacy-rules-236607.
[44] For a full discussion of relevant legislation, see Dempsey, J. X. and Flint, L. M. (2004), 'Commercial Data and National Security', *George Washington Law Review*, Vol. 72, 2003–04, pp. 1476–81. See also Federal Trade Commission (undated), 'FTC Consumer Response Center Fair Credit Reporting Act', www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf; and Electronic Privacy Information Center, 'EPIC - The Fair Credit Reporting Act', https://epic.org/privacy/fcra.
[45] See Davis Wright Tremaine LLP (2016), 'Data Breach Notification Summary', www.dwt.com/files/Uploads/Documents/Publications/State%20Statuets/BreachNoticeSummaries.pdf; and National Conference of State Legislatures (2017), 'Security Breach Notification Laws', www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[46] Electronic Privacy Information Center (EPIC), 'Electronic Communications Privacy Act (ECPA)', https://epic.org/privacy/ecpa/.

investigations amid charges of unreasonable claims of extraterritoriality.[47] Current rules and norms are barely keeping up with the rapid changes in technology, terrorist threats, and law enforcement and surveillance techniques.[48]

Data encryption

Another long-standing debate centred around encryption and turned far more intense following the request by the Federal Bureau of Investigation (FBI) that Apple help gain access to the mobile phone of one of the shooters who killed 14 and injured another 22 in San Bernardino, California, in 2015. Ultimately, the FBI said it gained access to the phone without Apple's help, but the controversy continues over whether firms storing data should grant access to intelligence or law enforcement authorities with a warrant, or whether keys to encrypted data should reside exclusively with data owners.[49] The issue resurfaced with the release on Wikileaks in February 2017 of purported CIA documents outlining broad efforts to break into mobile phones of all types.[50]

Snowden and the world

Most prominent in fuelling the debate, of course, were the Snowden revelations, which touched off a firestorm in the US – and around the world. The practices he revealed seem to have evolved in the wake of the 11 September 2001 terrorist attacks on the US, and they expanded in response to political pressures to track terrorists and technological developments that made broad collection possible. Among the more damaging blows to the transatlantic relationship were reports that personal mobile phones of foreign leaders were monitored and that US intelligence services may have conducted surveillance with the assistance of America's largest telecommunications and technology firms.[51] President Obama ordered a broad review of intelligence practices and concluded that many should be tightened to protect personal privacy. Significantly, following the outcry in Europe and elsewhere, he committed that the US government would explicitly protect the privacy of foreign citizens as well.[52] Obama continued to adjust this balance in an executive order signed just before his second term ended, but the debate will surely grow more heated under the Trump administration, which has suggested that tracking terrorist activity will supersede other considerations.[53]

[47] Ellingsen, N. (2015), 'The Microsoft Ireland Case: A Brief Summary', Lawfare, 15 July 2015, www.lawfareblog.com/microsoft-ireland-case-brief-summary.
[48] There are mounting unresolved issues, for example, over the US government's ability to track criminals and terrorists through data mining of commercial databases that may be public and semi-public databases. See Dempsey and Flint (2004), 'Commercial Data and National Security'.
[49] Even those who are comfortable with such back doors in the US worry about other less democratic governments requiring similar access to encrypted personal information. See Leetaru, K. (2016), 'Why The Apple Versus FBI Debate Matters In A Globalized World', *Forbes*, 2 March 2016, www.forbes.com/sites/kalevleetaru/2016/03/02/why-the-apple-versus-fbi-debate-matters-in-a-globalized-world/#63fbed922639T. The Obama administration issued a statement in 2016 that did not favour back doors, although the FBI and Department of Justice to some degree felt differently.
[50] Miller, G. and Nakashima, E. (2017), 'Wikileaks says it has obtained trove of CIA hacking tools', *Washington Post*, 7 March 2017, www.washingtonpost.com/world/national-security/wikileaks-says-it-has-obtained-trove-of-cia-hacking-tools/2017/03/07/c8c50c5c-0345-11e7-b1e9-a05d3c21f7cf_story.html?utm_term=.c7d7536c17f7.
[51] Even years later, German parliamentarians were holding hearings about US and German surveillance activities, hearing testimony from Chancellor Angela Merkel that 'spying among friends is not acceptable'. Moulson, G. (2017), 'Germany's Merkel testifies on alleged US eavesdropping', Associated Press, 16 February 2017, https://apnews.com/e384920d20d44f038d3f6a80a36b244f.
[52] See the full text of Presidential Policy Directive 28 at The White House (2014), 'Presidential Policy Directive – Signals Intelligence Activities', Office of the Press Secretary, 17 January 2017, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities; and President Obama's speech explaining the new policy, The White House (2014), 'Remarks by the President on Review of Signals Intelligence', Office of the Press Secretary, 17 January 2014, www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
[53] For a perspective on how these debates work their way through the US bureaucracy regardless of who is president, see Kaveh Waddell's interview with Susan Hennessey, managing editor of Lawfare, at Waddell, K. (2017), 'Why is Obama Expanding Surveillance Powers Right Before He Leaves Office', *The Atlantic*, 13 January 2017, www.theatlantic.com/technology/archive/2017/01/obama-expanding-nsa-powers/513041/.

Regulating data and boosting commerce

One important by-product of the Snowden affair was the fresh attention it drew to the prominence of technology and digital commerce within the US economy, and the difficult issues around its own use and analysis of data. In announcing tighter requirements on US intelligence activities, President Obama declared that they also 'take into account our trade and investment relationships, including the concerns of American companies'.[54] He also ordered a White House report on the challenges of big data analytics that would propose ideas on 'international norms' that would 'promote the free flow of information in ways that are consistent with both privacy and security'.[55] By May 2016, Congress had established a bipartisan working group on the economic potential of the internet of things and the potential challenges that might require legislation.[56]

[54] See The White House (2014), 'Remarks by the President on Review of Signals Intelligence'.
[55] The White House (2015), *Big Data: Seizing Opportunities, Preserving Values*.
[56] Latta, B. and Welch, P. (2016), 'The Internet of Things has the potential to be the engine that powers our economy for decades to come', *The Hill*, 31 May 2016, http://thehill.com/blogs/congress-blog/technology/281495-the-internet-of-things-has-the-potential-to-be-the-engine-that.

4. European Approaches to Data Regulation

If the US debate over data policy is often a struggle to balance the protection of national security and personal privacy, the political setting in Europe is more complex and the trade-offs are sometimes different. To be sure, security and privacy concerns dominate, but they are further shaped by different institutional structures and responsibilities as well as some instincts to protect Europe's technology industry in its struggle against US giants. In some European policy circles, there is genuine anxiety that the continent is falling behind in digital technology and artificial intelligence, with potentially significant consequences for its long-term competitiveness.

Institutional differences

While responsibilities for privacy, national security and economic growth usually rest within different parts of the US government, the most important decisions involve the White House weighing the conflicting imperatives.[57] The picture in Europe is far more complicated. Above all, the EU maintains responsibility over issues of privacy, data protection and the digital single market, while law enforcement, anti-terrorist and intelligence matters are handled almost exclusively by the member states. In contrast to a variety of legal and regulatory acts that protect privacy in the US, the EU derives clear responsibilities in this area from the Charter of Fundamental Rights of the EU, and privacy protections are incorporated into the 2009 Lisbon Treaty.[58] The 1995 Data Protection Directive sets out clear requirements that citizens must give specific consent for the collection and use of personal data and that they have a right to hold organizations accountable for misusing or inadequately protecting their data.[59] Given the rapid changes in technology and the economy, the EU has updated this directive with the GDPR, which takes effect in May 2018. The new regulation reinforces the principle that data should only be gathered under strict control and for legitimate purposes, extends rights to individuals on the portability of their data, and reinforces protections regarding information disseminated online.[60]

Member state differences

While these restrictions pose their own set of issues for firms, there are further complications from their interpretation and implementation. In many instances the rules are enforced by the data

[57] Kerry, C. F. (2016), 'Bridging the internet cyber gap: Digital policy lessons for the next administration', Center for Technology Innovation at Brookings, 7 October 2016, www.brookings.edu/research/bridging-the-internet-cyber-gap-digital-policy-lessons-for-the-next-administration/.
[58] See Articles 7 and 8, *Official Journal of the European Communities* (2012), 'Charter of the Fundamental Rights of the European Union', www.europarl.europa.eu/charter/pdf/text_en.pdf.
[59] See 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data', Official Journal L 281, 23/11/1995 P. 0031 – 0050, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML; and 'EU Data Protection Directive (Directive 95/46/EC)', http://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC.
[60] Mantelero, A. (2013), 'The EU Proposal for a General Data Protection Regulation and the roots of the right to be forgotten', *Computer Law and Science Review*, 29 (2013), pp. 229–35. This broad regulation has been further supplemented by the Directive on Privacy and Electronic Communications, which provides for protection of data over public networks. The European Commission has also approved a proposed update in January 2017 in a Regulation on Privacy and Electronic Communication. See European Commission (2017), 'Digital privacy', https://ec.europa.eu/digital-single-market/en/online-privacy. For the proposed ePrivacy Regulation, see European Commission (2017), 'Proposals for an ePrivacy Regulation', https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

protection authorities in each member state.[61] Google's privacy rules have been under separate scrutiny by regulators in some EU states. To add to the complexity, while there are unified privacy laws in Germany, each of its 16 federal states has data privacy officials responsible for enforcement; they have been known to approach the job with varying degrees of stringency.[62] If this were not enough, there have also been complaints that these local agencies are understaffed and undertrained for the task.[63]

Judicial rulings

If there is uncertainty around the implementation of EU rules by each member state, European courts have been adding to the confusion. Most prominently, the European Court of Justice (ECJ) backed what is famously known as the 'right to be forgotten' following a claim by a Spanish citizen that his privacy had been infringed by a newspaper and Google's search engine, which continued to post links to the newspaper's reports about a long-settled bankruptcy proceeding. The court ruled that under certain circumstances, citizens could ask search engines to remove links that violated their privacy even if the data are located on a server in the US.[64] While the decision clarified that such decisions had to be balanced against other rights such as freedom of expression, it injected yet another source of confusion into rules about what data can be kept and where.

Digital single market

Alongside these efforts to protect privacy, European authorities have been working on new rules for a 'digital single market', which would enhance opportunities in e-commerce, cloud computing, borderless mobile data connectivity and government services.[65] The most recent strategy, published in 2015, has a long list of goals that include harmonizing rules on cross-border digital purchases, ending practices that allow websites to charge different prices to customers in different jurisdictions, and promoting common standards and interoperability for activities such as e-freight and energy metering.[66]

[61] Newman, A. L. (2011), 'Watching the Watchers: Transgovernmental Implementation of Data Privacy Policy in Europe', *Journal of Comparative Policy Analysis: Research and Practice*, 13:2, 181–194, DOI: 10.1080/13876988.2011.555997.
[62] For data protection authorities in different EU states, see European Commission (undated), 'Data protection bodies', http://ec.europa.eu/justice/data-protection/bodies/index_en.htm. See Dautlich, M., Kauffmann, M. and Appt, S. (2013), 'Data protection enforcement in UK, France and Germany explained', Out-Law.com, 5 July 2013, www.out-law.com/en/articles/2013/july/data-protection-enforcement-in-uk-france-and-germany-explained/.
[63] European Union Agency for Fundamental Rights (2010), 'Data Protection in the European Union: the role of National Data Protection Authorities', Luxembourg: Publications Office of the European Union, http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf.
[64] For the legal history, see Mantelero (2013), 'The EU Proposal for a General Data Protection Regulation and the roots of the right to be forgotten', pp. 229–35. For more on the Spanish case itself, see European Commission (2014), 'Facts sheet on the right to be forgotten', http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.
[65] See European Commission (2017), 'The Digital Competence Framework', EU Science Hub, https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework; and European Parliament (2017), 'The ubiquitous digital single market', Fact Sheets on the European Union, www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_5.9.4.html.
[66] European Council (2017), 'Digital single market for Europe', www.consilium.europa.eu/en/policies/digital-single-market-strategy/.
The tensions are everywhere, including for example in widely available mapping data, which can be analysed through advanced data-mining techniques to reveal personal information that violates data privacy regulations. Van Loenen, B., Kulk, S. and Ploeger, H. (2016), 'Data protection legislation: A very hungry caterpillar; The case of mapping data in the European Union', *Government Information Quarterly,* 33 (2016) pp. 338–345.

US–EU competition

Underlying many of these challenges is concern in Europe about the domination of new data technologies – whether hardware, software or services – by US companies. In cloud storage alone, the top four firms in Western Europe are American (Microsoft, Google, IBM and Amazon).[67] While European citizens and politicians are uncomfortable with US government surveillance practices, some are even more squeamish about so much of their data being entrusted to large American firms. This prompted the EU, at least in part, to respond with its own secure cloud initiative.[68] US technology giants – whether they produce hardware (Cisco, Apple), software (Microsoft, Google) or simply gather data (Google, Facebook) – have come under increasing pressure. In one survey after the Snowden leaks, two-thirds of non-US firms surveyed said they had halted or planned to reduce spending with US internet service firms.[69] While German companies fret that their country is falling behind in the digitization of industry, the German government has, for example, proposed guidelines that require data providers to store all government data on servers in Germany.[70] Indeed, one measure of this discomfort is evident in the scale and scope of the new GDPR itself. Firms estimate they may have to spend five to 10 times the billions of euros they spent on Y2K compliance in order to operate within the new framework. While its provisions apply to US and European firms alike, violations can result in fines of up to 5 per cent of global revenues, which is especially painful for the non-European giants.[71] In the words of EU Commissioner Gunther Oettinger: 'The Americans are in the lead. They've got the data, the business models and so the power.'[72] Analysts, meanwhile, have urged policymakers to resist knee-jerk reactions and to 'protect data privacy in a way that keeps markets open and Europe's services exporters competitive'.[73]

[67] Schechner, S. (2016), 'U.S. Tech Firms Dominate Cloud Services in Western Europe', *Wall Street Journal*, 4 August 2016, www.wsj.com/articles/u-s-tech-firms-dominate-cloud-services-in-western-europe-1470303004.
[68] European Commission (2012), 'Unleashing the Potential of Cloud Computing in Europe', 27 September 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF; and European Commission (2013), 'What does the Commission mean by secure Cloud computing services in Europe?', 15 October 2013, http://europa.eu/rapid/press-release_MEMO-13-898_en.htm.
[69] Taylor, P. (2013), 'Cloud computing industry could lose up to $35 billion on NSA disclosures', *Financial Times*, 5 August 2013, www.ft.com/content/9f02b396-fdf0-11e2-a5b1-00144feabdc0.
[70] See Chazan, G. (2017), 'Why Germany Needs to Accelerate into the Digital Fast Lane', *Financial Times*, 25 January 2017, www.ft.com/content/31469796-dcd1-11e6-9d7c-be108f1c1dce; and Lee-Makiyama, H. and Bauer, M. (2015), 'The Bundes Cloud: Germany on the Edge to Discriminate Against Foreign Suppliers of Digital Services', European Centre for International Political Economy, September 2015, http://ecipe.org/publications/the-bundes-cloud-germany-on-the-edge-to-discriminate-against-foreign-suppliers-of-digital-services/.
[71] Titcomb, J. (2016), 'We mustn't let Brexit open up a chasm with Europe on data protection', *Telegraph*, 30 June 2016, www.telegraph.co.uk/technology/2016/06/30/we-mustnt-let-brexit-open-a-chasm-with-europe-on-data-protection/.
[72] Fairless, T. (2015), 'Europe's Digital Czar Slams Google, Facebook', *Wall Street Journal*, 24 February 2015, www.wsj.com/articles/europes-digital-czar-slams-google-facebook-over-selling-personal-data-1424789664.
[73] Lee-Makiyama, H. and Legrain, P. (2017), 'Open Up: How to Fix the Flaws in the EU's Digital Single Market', Open Political Economy Network (OPEN), January 2017, www.opennetwork.net/wp-content/uploads/2017/01/OPEN-Open-Up-DSM-final.pdf.

5. The Transatlantic Dialogue on Data

These differing sensitivities to privacy and national security, contrasting legal traditions, misaligned institutional structures and competing commercial interests have all contributed to an increasingly difficult conversation over how best to monitor, protect and regulate transatlantic data. One sign of the mismatch is that for all the concern about the protection of European data in the US, few Americans have called for better protection of US data in Europe. They may take some comfort in the fact that the firms that dominate data storage are American, but the situation may also reflect different sets of preferences. So far, the conversation has mostly yielded stop-gap measures that remain tenuous amid rapid changes in technology, politics and jurisprudence. Companies that simply accumulate data in the normal course of business face mounting uncertainties about how they must store and protect such data. Firms that have embraced the potential of actively managing and analysing data for innovative commercial purposes find themselves operating in a particularly treacherous political and regulatory environment. The conflicting rules and uncertainty not only constrict their own potential profitability, but threaten to limit or undermine the potential benefits to consumers and regulators as well.

Demise of Safe Harbour

The Safe Harbour framework was an effort to reconcile the differences in the US and European approaches. Concluded in 2000 following painstaking negotiations, Safe Harbour permitted several thousand companies to move data collected in Europe to the US if they certified they could provide an adequate level of protection.[74] That all came tumbling down in the wake of the Snowden disclosures when Max Schrems, an Austrian graduate student, claimed that Ireland's data protection authority had failed to protect his data when it allowed Facebook to store the data on servers in the US. The premise was that the US servers were vulnerable to interception by US intelligence services, thus violating European citizens' rights.[75] Ultimately, the ECJ found in his favour, sending firms scrambling to identify alternative ways to comply. Some resorted to new storage in Europe, while others faced fresh risks of litigation.[76] US authorities did what they could to engage in the European debate productively, but were always wary that forceful intervention from Washington risked triggering counterproductive resentment. Nevertheless, the State Department sought to rebuff the narrative taking shape around the ECJ's decision, insisting that the US 'does not and has not engaged in indiscriminate surveillance of anyone, including ordinary European citizens'.[77] Even the general counsel for the Office of the Director of National Intelligence, Robert Litt, felt compelled to publish a detailed rebuttal of some of the court's assertions. Remarkably, he revealed that in 2014 US intelligence services had 90,000 people under surveillance among a population of 3.2 billion

[74] Export.gov (2013), U.S.-EU Safe Harbor Framework Documents, http://2016.export.gov/safeharbor/eu/eg_main_018493.asp.
[75] Darcy, S. (2015), 'Battling for the Rights to Privacy and Data Protection in the Irish Courts', *Utrecht Journal of International and European Law*, 31(80), 131, DOI: http://dx.doi.org/10.5334/ujiel.cv.
[76] Delgado, C. (2016), 'The Demise of Safe Harbor and Rise of Privacy Shield', *FreedomWorks*, 2 April 2016, www.freedomworks.org/content/demise-safe-harbor-and-rise-privacy-shield.
[77] Robinson, D. (2015), 'U.S. attacks EU judge's inaccurate assertions on net surveillance', *Financial Times*, 28 September 2015, https://next.ft.com/content/b9b3e866-65ec-11e5-97d0-1456a776a4f5.

internet users – or 0.0028 per cent of the online population.[78] Some US officials have privately argued that EU citizens' data are far better protected on servers based in the US than in Europe itself. Not only is the cybersecurity likely to be better, but the restrictions against US government surveillance on US territory are far more robust than limitations on some European intelligence services in their own countries.[79]

Privacy Shield

With large flows of transatlantic trade at risk, following more than two years of negotiations, the US Department of Commerce and European Commission hammered out a new agreement called Privacy Shield, which included a more robust set of protections for European data.[80] Industry estimated that the new arrangement protects $260 billion in transatlantic commerce.[81] European officials have stressed that the new regime gives significantly greater protection to European personal data than its predecessor, stressing stronger obligations for US firms and redress mechanisms for EU citizens.[82] Still, the critics have not been assuaged and further court challenges to transatlantic data movements are in the works.[83] Particularly vulnerable are inter-corporate legal arrangements based on 'model clauses' or 'binding agreements' that, distinct from Privacy Shield, allow for data transfers out of the EU not only to the US, but to jurisdictions like China and Russia where privacy protections are far more questionable.[84] Other cooperative agreements to fight terrorism also came under attack during these often emotional exchanges, especially the Passenger Name Record Agreement and the Terrorist Finance Tracking Programme, which involved sharing European data with US law enforcement officials. A separate US–EU 'Umbrella' Data Privacy and Protection Agreement, which establishes the basis for law enforcement data transfers, has helped steady the cooperation. The EU insisted on new US law to provide limited paths for some EU citizens to seek redress in the event of their data being mishandled in the US. Still, challenges remain in Europe's courts and parliament, even as the Trump administration's views of the agreement have yet to be clarified.[85]

[78] These were all approved under Section 702 of the Foreign Intelligence Surveillance Act or the programme that Snowden revealed as 'Prism'. See Litt, R. (2015), 'Europe's court should know the truth about US intelligence', *Financial Times*, 5 October 2015, https://next.ft.com/content/90be63f4-6863-11e5-a57f-21b88f7d973f.

[79] As one commentator points out: 'One would be hard pressed to find the differences between core provisions of the new surveillance law in France – which includes the controversial practice of using algorithms to analyse metadata to identify potential suspects – and those at work in America. France's high court has found this practice constitutional, even if some prior decisions from the ECJ would suggest such practices do go against European legislation.' See Morozov, E. (2015), 'Worldwide fight over personal data has barely begun', *Financial Times*, 8 October 2015, www.ft.com/content/683f8cc0-6da7-11e5-aca9-d87542bf8673.

[80] For the EU documents related to Privacy Shield, see European Commission (2016), 'The EU-U.S. Privacy Shield', http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm. US firms that have been certified are listed at www.privacyshield.gov/list.

[81] Scott, M. (2016), 'Europe Approves New Trans-Atlantic Data Transfer Deal', *New York Times*, 20 July 2016, www.nytimes.com/2016/07/13/technology/europe-eu-us-privacy-shield.html?_r=0. For a detailed analysis, see Hufbauer, G. C. and Jung, E. (2016), 'The US-EU Privacy Shield Pact: A Work in Progress', Peterson Institute for International Economics, August 2016, PB 16–12, https://piie.com/publications/policy-briefs/us-eu-privacy-shield-pact-work-progress.

[82] European Commission (2016), 'European Commission launches EU-US Privacy Shield: stronger protection for transatlantic data flows', press release, 12 July 2016, http://europa.eu/rapid/press-release_IP-16-2461_en.htm. For a more detailed analysis, see Klosek, J. (2016), 'EU-US Privacy Shield Formally Adopted', Alert, Goodwin Procter LLP, 11 August 2016, www.goodwinlaw.com/viewpoints/2016/08/08_11_16-eu-us-privacy-shield-framework-adopted.

[83] Cahill, K. (2017), 'Storm clouds gather for US-EU Privacy Shield data deal', *Computer Weekly*, 25 April 2017, www.computerweekly.com/opinion/Storm-clouds-gather-for-US-EU-Privacy-Shield-data-deal.

[84] The most prominent case is brought by the very same Max Schrems.

[85] Stupp, C. (2016), 'Commission's 'Umbrella Agreement' with US under fire from MEPs', EurActi.com, 17 February 2016. The Trump administration has given early signs of support for 'Privacy Shield', but it has signalled far more aggressive intentions on balancing anti-terrorist activities with civil rights. See Drozdiak, N. (2017), 'Trump Administration to Protect European Privacy Rights, U.S. Tells EU', *Wall Street Journal*, 27 February 2017, https://blogs.wsj.com/brussels/2017/02/27/trump-administration-to-protect-european-privacy-rights-u-s-tells-eu/.

Brexit implications

If the picture were not confusing enough, there are further complications for firms operating out of Britain. Its precise path towards exiting the EU remains unclear, but its new status will likely leave it outside mandatory coverage of the EU's GDPR. The problem is that firms with UK and EU operations will need to adjust to whatever new regulations develop locally, while at the same time needing to comply with the expansive requirements of the EU regulation.[86] British governments have sometimes stressed national security concerns over privacy sensitivities more than the rest of the EU has done, a position partly reflecting Britain's own experience with domestic terrorism and its close intelligence cooperation with the US. The choices for firms will be especially difficult since the UK's recent adoption of the Investigatory Powers Act 2016, which codifies intelligence bulk data collection and interception.[87] British firms operating in the EU will need to convince continental authorities that they are protecting personal data to EU standards, which may be increasingly difficult as the new UK regime takes shape.

Trade regimes

Efforts to regulate the movement of data across the Atlantic have also been undertaken through trade negotiations. US trade negotiators have been generally pleased with the digital chapter and related provisions in the Trans-Pacific Partnership (TPP), which was agreed with 11 other Pacific countries before the Trump administration withdrew in January 2017. The approach, which they have sought to introduce into discussion with Europe, attempts to strike a balance between the need for data protection and support for the free flow of commerce in an increasingly digital world. The 'Digital 2 Dozen' in the TPP is what former deputy US trade representative Robert Holleyman calls principles developed at his agency to protect the internet as a marketplace of ideas, goods and services. They also aim to restrict rules that require data localization or discriminate against foreigners.[88] These principles have been important in the conversations over the Trade in Services Agreement (TiSA) – which aims to cover 70 per cent of the world's trade in services, including the US and the EU, and to update rules that date back before the explosion of internet activity.

> The 'Digital 2 Dozen' ... [aims] to protect the internet as a marketplace of ideas, goods and services [and] restrict rules that require data localization or discriminate against foreigners.

These conversations, however, remain very difficult with the EU – both over TiSA and the potential free-trade agreement, the Transatlantic Trade and Investment Partnership (TTIP). Even before the Trump administration put US trade policy under review, negotiators had made little progress on data issues amid uncertainty over the implementation of the GDPR and the European Parliament's general

[86] The challenge is real for both large and small firms. See Ford, J. (2017), 'Digital banker fears Brexit will damage competition', *Financial Times*, 15 February 2017, www.ft.com/content/c689745a-ee0f-11e6-ba01-119a44939bb6.
[87] Taylor, E. (2016), '"Brexit" Could Put Data Sharing in Jeopardy', Chatham House Expert Comment, Royal Institute of International Affairs: London, 10 March 2016, www.chathamhouse.org/expert/comment/brexit-could-put-data-sharing-jeopardy.
[88] See Holleyman, R. (2016), 'The Trans-Pacific Partnership and the Digital Economy', Remarks by Deputy U.S. Trade Representative Robert Holleyman to the Commonwealth Club in San Francisco, 30 March 2016. See also Office of the United States Trade Representative (2016), 'The Digital Two Dozen', Executive Office of the President, https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2016/digital-2-dozen. This success notwithstanding, the US introduced a carve-out for some banking data to be stored locally at the insistence of the US Federal Reserve Board, which was concerned about its oversight functions. US negotiators had intended to reassert the principle of free data movement during TiSA negotiations, but these talks are likely to face a thorough review by the Trump administration.

distrust of US privacy protection. The grass-roots opposition to TTIP has magnified fears of private European data ending up in the hands of large US companies.[89] These opponents urge close review by courts and privacy authorities of any final agreement, and have denounced TTIP as a 'digital Trojan horse' for 'America's data giants'.[90] TiSA remains in limbo as well, at least in part due to European difficulties in devising a negotiating position that meets the requirements of EU data rules.[91]

[89] See https://endofsafeharbor.eu/, which also lists European tech firms it says do not cooperate with the National Security Agency.
[90] Chester, J. (2016), 'EU data protection rights at risk, new study shows', Center for Digital Democracy, 13 July 2016, www.democraticmedia.org/blog/eu-data-protection-rights-risk-through-trade-agreements-new-study-shows. See also Irion, K., Yakovleva, S. and Bartl, M. (2016), 'Trade and Privacy: Complicated Bedfellows', Institute for Information Law, University of Amsterdam, 13 July 2016, www.democraticmedia.org/sites/default/files/field/public/2016/dp_and_trade-web.pdf.
[91] Rupert Schlegelmilch, director of services and investment with the European Commission's Directorate General for Trade: 'It is clearly an economic issue but … we do not want to sacrifice the fundamental right on data protection by doing something irresponsible.' Behsudi, A. (2016), 'Let's get Ready to Lumber', Politico Morning Trade, 13 October 2016, www.politico.com/tipsheets/morning-trade/2016/10/lets-get-ready-to-lumber-216840.

6. A Transatlantic Charter for Data Security and Mobility

With Europe and America largely talking past each other on a crucial issue that is likely to become more complicated before any viable solutions come into view, aspirations for good policy must remain modest. Regulators on both sides have worked hard to reach closer alignment as their tireless efforts on the Privacy Shield and Umbrella agreements attest. These understandings may, in fact, endure if they can be reinforced or adjusted in regular reviews. Fundamentally, however, the problem lies in the fact that US and European citizens remain at best undecided – and more accurately, confused – about where to strike the balance between privacy and security. More challenging still is that the debate is playing out amid rapid technological change that has brought data collection, storage and analysis into all manner of commercial, industrial and personal activities. The possible individual and social benefits of sophisticated data analytics remain tantalizing, but the potential for both private and public abuse are much easier to foresee. This makes the challenge of setting the rules without throttling the potential all the more difficult.

Fundamentally, the problem lies in the fact that US and European citizens remain at best undecided – and more accurately, confused – about where to strike the balance between privacy and security.

Of course, the transatlantic debate on these issues has also taken place amid broader international efforts to establish rules and standards. The Organisation for Economic Co-operation and Development (OECD) updated its privacy guidelines in 2013 with proposals for mechanisms to enforce protections.[92] The Asia-Pacific Economic Cooperation (APEC) forum has tried to explicitly balance concerns for privacy with the importance of economic growth in its 'Cross-Border Privacy Rules System', encouraging businesses to develop sound data privacy practices in order to build trust among governments and citizens in the security of cross-border flows of personal information.[93] As the goods that cross international borders arrive increasingly with embedded operating software that is often updated and repaired remotely, the WTO has been studying these issues as well. One of the most vexing questions is how to decide if such deliveries should be governed more by the rules for goods or the rules for services.[94]

While these are important efforts, little could be more powerful than a single framework for digital regulation for both the US and Europe – the most digitized economies in the world. Detailed rules on the proper handling and protection of transatlantic data may be quite far off, but a common

[92] Organisation for Economic Co-operation and Development (2013), '2013 OECD Privacy Guidelines', www.oecd.org/internet/ieconomy/privacy-guidelines.htm.
[93] See Asia-Pacific Economic Cooperation (2011), 'Cross Border Privacy Rules System', www.cbprs.org/. APEC's 2004 'Privacy Framework' also attempts an explicit balance between protecting privacy and boosting free trade. See Asia-Pacific Economic Cooperation (2005), *APEC Privacy Framework*, APEC Secretariat: Singapore, www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx. At their 2016 summit, APEC leaders declared a commitment to 'privacy protection' and 'flexible frameworks'. See Asia-Pacific Economic Cooperation (2016), '2016 Leaders' Declaration', Lima, Peru, 20 November 2016, www.apec.org/Meeting-Papers/Leaders-Declarations/2016/2016_aelm.
[94] Porges, A. and Enders, A. (2016), 'Data Moving Across Borders: The Future of Digital Trade Policy', The E15 Initiative, April 2016, www.ictsd.org/sites/default/files/research/E15-Digital%20Economy-Porges%20and%20Enders-Final.pdf.

approach would help smooth the path to more durable and coordinated regulation. Industry groups are naturally engaged in efforts to promote common standards or friendlier policies for their own firms, whether on net neutrality or data portability. Other proposals would help make transatlantic data rules more aligned.[95] Many of these ideas, however, are both too specific and too aspirational. A more concrete, yet more achievable, mechanism for consultation and framework for agreement would be a 'Transatlantic Charter for Data Security and Mobility' between the US and the EU. Such a document might establish general principles that governments would observe as they analyse and deploy specific rules on data collection, handling and analysis. It would also encourage constructive engagement in these decisions from industry. While final agreement on such a charter by US and European policymakers would represent a signal achievement, the effort of seeking consensus on basic principles can in itself be helpful in establishing trust among governments that regulate data and companies that increasingly depend on data.

Principles for cooperation

While US and EU authorities are already committed to an open and accessible internet, broad availability of government databases and the free movement of data, such shared values bear repeating in the context of the dynamic and complex issue of data rules. The challenges that will need to be resolved in the framework of this charter will be difficult and emotional. Both sides should explicitly reaffirm their shared aspirations.

As the authorities commit to as few restrictions on data movement as possible, they should also acknowledge that any rules in the realm of data security and mobility will require difficult compromises between the requirements of national security, personal privacy and economic freedom. Authorities should also commit to undertake an analysis of these trade-offs for any new rule or law under consideration. Innovation and experimentation involve risks to privacy and national security. Protecting privacy will inevitably complicate the work of law enforcement and data innovators. Absolute security is all but impossible without abandoning privacy and innovation entirely. Policymakers will not all make the same choices and their regulations will never be identical, but they should at least be required to acknowledge the trade-offs they faced and justify their final decisions.

Each side should also agree to mutual consultations on any data rules or regulations that might affect the firms or citizens of the other. This would include explaining how such a rule aligns with the framework of the other side and making specific efforts to minimize any contradictions. Parties to the charter would also pledge to avoid any regulation that would have the effect of imposing data localization requirements or discriminatory rules.

Mechanisms for cooperation

The charter would also establish a series of consultative actions between US and European authorities and with industry.

[95] For one especially thoughtful set of proposals, see Kennard, W. E., Bildt, C. and Burwell, F. (2016), 'Building a Transatlantic Digital Marketplace: Twenty Steps Toward 2020', The Atlantic Council, April 2016, www.atlanticcouncil.org/publications/reports/building-a-transatlantic-digital-marketplace-twenty-steps-toward-2020.

The charter would call for broader official dialogues on key elements of data regulation to help coordinate or supplement existing mechanisms – for example, within the context of Safe Harbour. These might include conversations between financial or industrial regulators to expand their understanding of the transatlantic data debate and its implications for their industries. Engagement could also focus on cross-sectoral issues such as the challenges around establishing data 'ownership' or the purchase and sale of databases themselves. Most important would be the establishment of more extensive mechanisms to engage US and European legislators, since they are often most caught up in the emotional politics around these issues without enough background on the commercial and international implications of the debate.

Engaging the private sector and interest groups

Officials are usually in frequent conversation with the industries they regulate, but the charter might also encourage more formal consultations with commercial and industrial leaders, who might be more inclined to cooperate with governments in a crisis if they are having regular conversations on data protection, encryption and privacy. While firms and interest groups would not be formal parties to the charter, they should be encouraged to endorse its principles.

Firms might be called upon to develop similar data charters for their own industries. These would establish principles and commitments specific to financial services, telecommunications or manufacturing, since each sector relies on different types of data, which trigger different concerns. Industry-level charters might also include codes of conduct, or broad practices like a 'right to explanation', which is already part of European rules requiring firms to explain algorithms that may restrict a consumer's choice. Banks could establish their own principles on the collection, protection and usage of customer data. Industrial firms could develop standards that would make it easier for data from different industrial components to be analysed by the same software. Firms might also develop a code of ethics for data professionals, which would commit employees who handle and analyse data to a 'due care' standard, whether their work involves personal, industrial or governmental data. This would involve commitments to use the data only in ways that the client has intended, to take all reasonable measures to protect the data, and to answer all reasonable client requests about how the data are stored and used. In some cases, given the complexities of the issues involved, industries might encourage the development of third-party certification. Just as firms like Morningstar offer ratings for mutual funds and UL (Underwriters Laboratories) provides expert testing for consumer products, independent analyses could assess how Google's latest algorithm or Siemens' industrial software meets concerns for reliability, privacy and security.

No doubt, a 'Transatlantic Charter for Data Security and Mobility' will take time to discuss and agree, especially if industry is drawn into the effort. Ideally, the initial conversations could be launched as part of the annual reviews of the US–EU Privacy Shield Agreement. From there, these principles could serve as the framework for agreed approaches within the G7, G20, APEC or even the WTO. As with so many policy efforts around complex issues, however, the journey may be as important as the destination. Engagement by EU and US officials on basic principles around data protection that recognizes the competing concerns for national security, privacy and economic growth would lay an important foundation for a more productive working relationship.

7. Conclusion

Recent elections in the US and Europe have triggered a reassessment of the transatlantic relationship regarding national security, trade, human rights and more. In the end, cooperation on these issues will likely continue simply because so many shared interests endure. Yet, the rapidly expanding torrents of data – whether commercial, personal or industrial – pose fresh challenges to these shared interests. There is potential for great expansion of productivity, as well as substantial weakening of traditional national security tools. There could be significant gains in government efficiency, as well as historic erosion of personal privacy and human rights. The choices are not simple for any government in its own jurisdiction given the rapid pace of technological change. They are all the more complex for lasting cooperation between US and European officials, whose choices are shaped by different cultures, political dynamics and institutional structures. Current consultations have helped shape a tenuous basis for cooperation amid emotional exchanges about espionage, protectionism and economic stagnation. More substantial engagement is essential, however, to avoid future regulatory regimes that strangle innovation or undermine political trust. A 'Transatlantic Charter for Data Security and Mobility' – as this paper proposes – will hardly lead to complete alignment on these questions, but it can help establish the framework for a debate that all too often lurches to extremes and risks damaging a fundamental alliance for global stability along with a fundamental driver of 21st-century economic progress.

Appendix: Elements of a 'Transatlantic Charter for Data Security and Mobility'

Establishing principles for cooperation

- Promote a free and open internet;
- Promote cross-border data flows;
- Refrain from imposing rules that discriminate against digital transfers from other countries;
- Ensure that government data be as open and available as possible;
- Design laws and regulations that provide the necessary protection of personal privacy and national security with the minimum restrictions on data movement and usage;
- Share explicit analysis of the trade-offs between the policy goals of privacy, security and innovation; and
- Restrict rules regarding data localization to limited circumstances and after an analysis of the additional costs and assumed benefits.

Expanding cooperative mechanisms

- Establish emergency consultation mechanisms when either side wishes to raise concerns involving the proper protection or mobility of data;
- Invest in education that helps bridge the digital divide, and in public education around practices that keep data secure and mobile;
- Clarify rules around data ownership and database transactions; and
- Organize regular transatlantic dialogues on data policy and cybersecurity, especially among legislators who write the laws amid complex political dynamics.

Inviting private-sector engagement

- Encourage the development of sector-specific charters that include codes of conduct to outline best practices for data security and privacy protection, even while allowing flexibility for innovation;
- Encourage sectoral charters to include a code of ethics for data professionals, outlining best practices to maximize the appropriate usage and protection of personal and industrial data;
- Encourage firms and industry groups to promote standardization and interoperability of data collection, security and transfer protocols; and
- Promote the consideration of third-party validation mechanisms or firms that will monitor and analyse data practices across an industry, offering independent opinions on data protection and the alignment of data usage with client expectations.

About the Author

Christopher Smart is the Whitehead Senior Fellow in the US and the Americas Programme at Chatham House and a senior fellow at the Harvard Kennedy School's Mossavar-Rahmani Center for Business and Government. He spent six years in the Obama administration as a senior policymaker for international economic affairs. As special assistant to the president at the National Economic Council and the National Security Council, he was principal adviser on trade, investment and a wide range of global economic issues.

From 2009 to 2013, he was deputy assistant secretary of the treasury, where he led the response to the European financial crisis and designed US engagement on financial policy across Europe, Russia and Central Asia.

Before entering government, he was director of international investments and managed emerging markets funds at Pioneer Investments in Boston. Following the collapse of the Soviet Union, he worked in Moscow, advising Russian government agencies on economic policy and financial market reform.

Acknowledgments

The author and Chatham House would like to thank all the supporters of the John C. Whitehead Fellowship for their input into this study – through the provision of both financial support and substantive advice. The author is also grateful for research support from Victoria Alsina Burges and Edward Cuipa, as well as for helpful comments and suggestions from Andrew Bailey, Oliver Burrows, Megan Doberneck, R. David Edelman, Anthony Gardner, Jevon Gibbs, Robert Holleyman, Adam Hunter, Robert Macdougall, Nicolas Miailhe, Mikko Niva, Jacob Parakilas, Courtney Rice, Marianne Schneider-Petsinger, Emily Taylor, Xenia Wickett and several other anonymous reviewers. Thanks also go to Mike Tsang and Jake Statham for their editing of this paper.

Independent thinking since 1920

Cover image: A data centre for T-Systems, a subsidiary of Deutsche Telekom, shown in July 2014.

Photo credit: Copyright © Thomas Trutschel/Photothek/Getty Images

ISBN 978 1 78413 232 3

This publication is printed on recycled paper.

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223