Challenges
Challenges

Just as digitization’s advance faces various barriers in both Europe and the United States, it also confronts societies on each side of the Atlantic with a host of legal, economic, societal and normative questions. Let’s look at these challenges.

Despite the remarkable advance of the transatlantic digital economy, various hurdles challenge the ability of the United States and Europe to take fuller advantage of digitalization.

Digital Divides

Each side of the Atlantic faces a divide between economic sectors pushing towards the digital frontier and those lagging behind. Table 4.1 illustrates this divide, and also highlights the fact that the same industries tend to be at the frontier — and lag behind — on both sides of the Atlantic. The fact that this sectoral divide is similar in Europe and the United States offers a basis for more concerted transatlantic efforts to exchange good practice to accelerate digitization of lagging sectors of the economy.

This sectoral division also highlights a second common challenge: the digital divide between large and small firms. Since large firms tend to be more digitized than small ones, countries whose average firm size tends to be smaller may be further away from capturing the full potential of digitization. This can be significant for a country like Italy, where large firms account for only about 30% of

---

**TABLE 4.1: DIGITAL LEADERS AND LAGGARDS IN EUROPE AND THE UNITED STATES**

<table>
<thead>
<tr>
<th>Europe’s economy</th>
<th>U.S. economy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High Digitization</strong></td>
<td><strong>Assets</strong></td>
</tr>
<tr>
<td>- ICT</td>
<td>- ICT</td>
</tr>
<tr>
<td>- Media</td>
<td>- Media</td>
</tr>
<tr>
<td>- Finance</td>
<td>- Finance</td>
</tr>
<tr>
<td><strong>Medium Digitization</strong></td>
<td><strong>Assets</strong></td>
</tr>
<tr>
<td>- Mining</td>
<td>- Manufacturing</td>
</tr>
<tr>
<td>- Real estate</td>
<td>- Wholesale trade</td>
</tr>
<tr>
<td>- Education</td>
<td>- Retail trade</td>
</tr>
<tr>
<td><strong>Low Digitization</strong></td>
<td><strong>Example sectors</strong></td>
</tr>
<tr>
<td>- Hospitality</td>
<td>- Hospitality</td>
</tr>
<tr>
<td>- Construction</td>
<td>- Construction</td>
</tr>
<tr>
<td>- Agriculture</td>
<td>- Healthcare</td>
</tr>
</tbody>
</table>

*Source: McKinsey Global Institute.*
employment, compared to countries like the United States and the United Kingdom, where large firms account for more than half of overall employment. Prioritizing efforts to encourage small-firm digitization could be particularly significant not only for Italy, but also for Europe, since microenterprises with fewer than ten employees make up 18% of employment in Europe, compared to only 8% in the United States.  

**Fragmented Markets**  
Europe’s fragmented markets and regulatory heterogeneity not only hamper Europe’s digital potential, they hold back the full promise of the transatlantic digital economy.

In and of themselves, platforms favor no one, they offer a level digital field of potentially global reach. Companies can prosper to the extent they are able to take advantage of such scale and related network effects. American and Chinese platform companies have been successful in part because their large domestic markets and relatively homogenous regulatory frameworks enable them to gain size and strength at home before venturing abroad. European companies, in contrast, have struggled to achieve scale and network effects, despite efforts such as the European Single Market and the Digital Single Market.

As we showed in chapter 2.2, e-commerce within individual European markets is growing exponentially, yet cross-border e-commerce across European borders still accounts for only a small fraction of the total. Different national regulatory environments have fractured European service markets in an era in which scale and seamless commercial flows are essential components of competitiveness. E-merchants seeking to conduct cross-border commerce in Europe cite fragmented legal, taxation, logistics and distribution systems, as well as the complexity of offering alternative payment methods, as among the most difficult barriers they must overcome. Just the cost of legal fees required to comply with different national regulations are estimated at 9,000 euros per country, so that an e-commerce retailer might face a total of a quarter of a million euros in additional costs simply to be present in all EU member state markets. This is prohibitive for small- and medium-sized companies, which stand to be among the greatest beneficiaries of the digital economy. 

Localization requirements are another prominent hurdle. Such barriers include policies that require the in-country location of data servers; policies that require local content or technologies; and government procurement preferences and standards that favor local companies. Such barriers can reduce market access, increase costs to firms, result in less efficient business processes, and present consumers with fewer choices at higher prices. Geo-blocking, which encompasses the blocking or modification of digital content (including offers of physical goods and services) based on a customer’s nationality or place of residence, is a glaring example of how national laws restrict businesses from serving customers across European borders.

Just within the EU alone, the Belgian think tank ECIPE has identified 22 data localization measures where EU member states impose restrictions on the transfer of data to other member states, and another 35 restrictions on data usage that could indirectly localize data within an individual member state. One result is that two-thirds of all demand for ICT-related services is sourced locally within each member state, while only 18% is sourced from the rest of the EU and only about 13% sourced from outside the EU. ECIPE estimates that if these localization measures were removed, EU GDP would increase by €8 billion a year (up to 0.06% of GDP), which is on par with the gains of recent free trade agreements (FTAs) concluded by the EU.

These challenges are not limited to Europe. In 2015, a European Commission survey found that only 37% of websites, including those in the United States, actually allowed cross-border customers to reach the final step before completing the purchase by entering payment details. Nevertheless, the hurdles seem highest in Europe.

The result of this fragmentation is visible in Europe’s low 10% worldwide share of “unicorn” technology companies with a valuation of $1 billion or more; the fact that more than half of European unicorns are now owned by American corporations; and that the EU’s largest technology unicorn, music-streaming service Spotify, has repeatedly signaled that it is prepared to move operations from Stockholm to the United States should the regulatory and business environment in the EU and Sweden stay unchanged.

These challenges, in turn, are accentuated by Europe’s varied reactions to the platform economy. For instance, Barcelona fined Airbnb for breaking local property rental laws, while Amsterdam passed legislation to encourage more local sharing services. Berlin banned short-term rental services like Airbnb, while Paris has allowed home owners to use apartment-sharing services to rent out their flats as long as they fulfill certain safety requirements. Uber had been outlawed in Germany until Frankfurt overturned a ban in September 2016. Portugal has come to the sharing economy regulation game later and has seemingly benefited from other countries’ missteps, on both ends of the spectrum. Recently, the country drafted a new rental law that will not only help Airbnb
and similar businesses grow, but also encourage home owners to register their property and — more importantly — pay taxes.12

Once again, Europe is not alone in this hodgepodge reaction; a number of U.S. cities and states have responded to platforms in a variety of ways. Nonetheless, due to Europe’s fragmented markets, such efforts add another level of complexity and uncertainty to cross-border digital commerce on the continent.

**Challenges to the Digital Single Market**

The EU has sought to address these issues with its Digital Single Market (DSM) initiative, which encompasses an ambitious regulatory overhaul made up of 16 initiatives in three areas. The first area tackles barriers to consumer and business access to digital goods and services across Europe. The second seeks establish a technical framework that can facilitate greater cross-border digital commerce and boost the EU’s network environment. The third seeks to improve growth opportunities for start-ups and other companies that are either challenged by, or in a position to benefit from, digital transformation and the need for improved digital skills. A set of additional initiatives have also been passed, including the General Data Protection Regulation (GDPR), new regulations on net neutrality, abolishing of roaming charges, and efforts to tackle geo-blocking.13

While these efforts show promise and generally point in the right direction, critics have identified three major concerns with the DSM strategy.

The first concern is the speed of law vs. speed of light problem: legislative implementation lags woefully behind fast-moving digital developments. This is not a problem exclusive to the EU, but the need to harmonize legislation not only within EU member states but among them adds an additional layer of complexity and a great deal more time to the legislative process.14 It also costs money. A European Parliament study noted that a number of rather substantial barriers within the EU could reduce the value of potential increased use to up to €18 billion in the shorter-term and up to €134 billion in the medium and longer term, depending on the scale of regulatory obstacles.15 EU-wide directives continue to face challenges of uneven implementation. For instance, despite the European Commission’s efforts to ban geo-blocking, online stores across the continent keep refusing customers from other countries, charging higher prices to foreign customers or creating virtual boundaries in some other way.16 The Commission has launched investigations to assess if certain online sales practices prevent, in breach of EU antitrust rules, consumers from enjoying cross-border choice and being able to buy consumer electronics, video games and hotel accommodation at competitive prices.17

The second concern is that the DSM strategy is focused almost exclusively on tackling digital barriers, whereas the main obstacles to the EU’s digital future are its non-digital barriers. Creating a genuine non-digital European Single Market is arguably the most fundamental precondition to facilitate structural economic change and to create a true cross-national DSM.18

The Single Market is both the bedrock of European integration and the EU’s most potent instrument to address the challenges and opportunities of the digital age. Yet in many ways it remains a dream unfulfilled. Regulatory barriers persist all across the Union, while subsidies, tax schemes and other arrangements protect relatively unproductive companies from competition. A more complete and vibrant Single Market would provide countries and companies with a stronger geoeconomic base in a world of continental-sized players. It would give EU countries greater opportunities to exploit their full comparative advantage, and would give EU companies new possibilities to restructure their activities on a pan-European scale.19

Third, the narrow focus on digital also forgoes the opportunity to use the current digital transformation to open up EU services markets. The services economy is the EU’s biggest untapped source of jobs, economic growth, and digital transformation. While the EU-wide Services Directive has helped to forge a more coherent approach to services within the EU, it is not fully implemented, and excludes such critical areas of potential innovation and productivity growth as financial services, health, employment and social services. One study found that if the Services Directive were fully implemented, it could deliver more than 600,000 new jobs and boost GDP growth in the EU by up to 1.5%. And if services competition in the eurozone was raised to U.S. levels, the European Central Bank estimated that services sector output could be increased by 12%. Since the digital economy is integrally linked to the services economy, a Services Single Market would accelerate the Digital Single Market as well. Moreover, a true Single Market in Services would also position the EU’s biggest untapped source of jobs, economic growth, and productivity growth as financial services, health, employment and social services. One study found that if the Services Directive were fully implemented, it could deliver more than 600,000 new jobs and boost GDP growth in the EU by up to 1.5%. And if services competition in the eurozone was raised to U.S. levels, the European Central Bank estimated that services sector output could be increased by 12%. Since the digital economy is integrally linked to the services economy, a Services Single Market would accelerate the Digital Single Market as well. Moreover, a true Single Market in Services would also position the EU well internationally, since the EU is a world-class leader in services trade and investment.20

**From Cold War to Code War**

Every day, millions of cyberattacks are launched against targets in Europe and the United States, as well as in
many other countries. The Pentagon alone reports more than 10 million efforts at intrusion each day.\textsuperscript{21} Germany’s army was targeted 284,000 times by cyber attacks in the first three months of 2017.\textsuperscript{22} Each side of the Atlantic is challenged by cyber threats and what Alec Ross has dubbed “the weaponization of code.” The pervasive nature of the internet, together with the proliferation and democratization of digital technologies, has created a breathtaking set of vulnerabilities.\textsuperscript{23} Cyberattacks can be directed from one country to another, from a country to a company or a company to a country. Digitally-empowered individuals or crowd-sourced hackers, often with no return address, can cause as much damage as conventional military forces. 10 years ago, malicious digital activities did not register at all on the list of major threats to U.S. national security compiled by the Director of National Intelligence. In 2015, they ranked first.\textsuperscript{24}

Russian cyber-hacking of the Democratic National Committee in the United States is a recent and emblematic example of such attacks. But Russian hackers have also attacked the German Bundestag, France’s TV5 Monde and Poland’s Warsaw stock exchange. In 2007 Estonia was subjected to distributed denial-of-service attacks for weeks following a dispute with Russia about moving a World War II memorial to Soviet soldiers, and its Baltic neighbors Lithuania and Latvia have also been targeted by escalating cyberattacks. Georgia and Ukraine were attacked in similar fashion during Russia’s 2008 and 2014 invasions of these two countries. In many ways, Ukraine has in fact become a training laboratory for novel attack techniques on critical infrastructures that could be used in other countries; since 2015 the country’s power facilities, its national railway system and the Ministry of Finance have all been subject of attacks.\textsuperscript{25}

“The world has left the Cold War behind only to enter into a Code War,”\textsuperscript{26} notes Ross. NATO allies have determined that cyber defense is integral to the Alliance’s core task of collective defense, have recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea, and have initiated collaboration with the European Union and with industry. The United States and a number of European nations have established their own cyber commands, and the United States and the EU have each adopted cyber security strategies to address these challenges.\textsuperscript{27} These efforts, however, are still proving insufficient to the challenges. After Russia’s interference with the 2016 U.S. election, for instance, President Barack Obama felt the need to reclassify American elections as a ‘critical infrastructure’ warranting protection under U.S. Homeland Security guidelines. Yet government weather forecasting and GPS satellites, which are crucial to protect and enable critical infrastructure, are not yet included. NATO nations have agreed to prioritize seven baseline requirements for greater resilience, including to digital threats, yet they are being addressed on a country-by-country basis, thus ignoring the deep connections binding European national infrastructures to one another and the reality that resilience efforts, to be effective, must be shared — not only by public authorities, but also in partnership with the private sector, which owns much of the West’s critical infrastructure.\textsuperscript{28}

Public-private resilience partnerships are especially urgent because U.S. and European companies are the world’s leading targets of cyberattacks by states, terrorists and criminals.\textsuperscript{29} Malware is becoming ubiquitous, and ransomware attacks, where companies are forced to pay ransoms to avoid losing data or having systems shut down, have become mainstream. In recent years hackers have compromised more than 500 million Yahoo accounts, 117 million LinkedIn user emails and passwords, and 85 million accounts from the video sharing platform Daily Motion.\textsuperscript{30} Ninety percent of Citibank’s networks across North America were taken down by a disgruntled employee.\textsuperscript{31} The list goes on. According to Gemalto’s Breach Level Index (BLI), of the 1.4 billion data records lost or stolen from corporations worldwide in 2016, over 82% occurred in the United States and in Europe.\textsuperscript{32}

**U.S.-EU Differences: Privacy, Hate Speech, and Intellectual Property**

These examples underscore that the United States and Europe face a number of common challenges in the digital world. Yet the transatlantic digital economy is also held back by basic EU-U.S. differences on a range of issues, including privacy and personal data, rules regarding hate speech and fake news, and intellectual property protection.

**Privacy.** While the EU and the United States each protect privacy and personal data, their approaches in how to safeguard these rights differ in some respects. The EU’s revised General Data Protection Regulation, which will come into force in 2018, replaces 28 different national laws with one single set of rules for data protection, sharing and privacy in Europe’s Digital Single Market. The United States, in contrast, has no single, comprehensive federal (national) law regulating the collection and use of personal data. Instead, a collection of federal and state laws and regulations reigns, supplemented by an additional thicket of self-regulatory guidelines and frameworks by governmental agencies and industry groups that are considered “best practices” and that are increasingly being used as tools for regulatory enforcement.\textsuperscript{33} These differing legal frameworks can
cause transatlantic frictions, even though each party is committed to protecting privacy and personal data.

In recent years the United States and the European Union have struggled to craft agreed procedures that protect national security in ways that respect basic human rights. In January 2014, in the wake of the Snowden leaks and with the U.S. intelligence community under intense pressure from critics at home and abroad, President Obama issued Presidential Policy Directive 28 (PPD 28), which extends privacy protections to non-U.S. citizens should their personal data be obtained incidentally as part of U.S. surveillance targeting other individuals.34

Despite this promise, in 2015, the European Court of Justice (ECJ) invalidated a basic U.S.-EU agreement known Safe Harbor, which at the time was one of the primary ways that U.S. and EU companies could legally transfer commercial data on EU citizens outside of the EU. The ECJ’s invalidation of the agreement caused significant uncertainty for U.S. businesses operating in Europe, particularly small businesses that could not readily afford to build alternative legal channels for transferring data.

To address this, the United States and the EU negotiated a new agreement with the EU, known as the Privacy Shield, to replace the Safe Harbor agreement. The Privacy Shield is currently in effect, and thousands of U.S. and EU companies have signed up to it. The main points of the agreement include stronger obligations on companies in the United States to protect the personal data of EU citizens and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission; clearer conditions, limitations and oversight regarding personal data transfers; several redress possibilities to ensure effective protection of EU citizens’ rights; and an annual joint review mechanism.35

The European Commission has committed to defending the Privacy Shield before the ECJ, but both its ability and willingness to do so depend on the U.S. maintaining its privacy commitments, most of which are currently contained in U.S. law, particularly the USA Freedom Act and the Judicial Redress Act. Both are important foundations for the new Privacy Shield, as is PPD 28.

A related agreement is the U.S.-EU Umbrella Agreement protecting personal information exchanged as part of law enforcement cooperation. This includes information on suspects and convicted persons, but also innocent victims and witnesses. The Umbrella Agreement, which came into force on February 1, 2017, represents a common transatlantic privacy framework based on high standards.36

Another foundational element is Title VII, Section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA) Amendments Act, which will expire on December 31, 2017 unless Congress acts to extend the law. Section 702 allows warrantless surveillance of non-U.S. citizens believed to be outside of the U.S., and has provided the authority for the PRISM and UPSTREAM surveillance programs that enable interception of high volumes of internet data and telephone traffic, which have become so controversial in U.S.-EU relations. Surveillance under Section 702 was at the heart of the ECJ’s decision to strike down the Safe Harbor arrangement.37

Various stakeholders, particularly in Europe, have been critical of the oversight mechanisms for privacy violations and what they believe to be inadequacies in the limitation on collection, access and use of personal data.38 They argue that the U.S. is not fully compliant with all of its commitments under Privacy Shield, including not having a permanent independent ombudsperson in place.39 They also argue that there are many ways the U.S. could reform Section 702 to better protect human rights without undermining the security of U.S. citizens or others around the world. Others, particularly in the United States, are concerned that such limitations could endanger national security. As of this writing, the balance is holding. Yet if these foundational elements fall away, the tortuous issues that have plagued U.S.-EU relations will be back on the table, chilling the transatlantic digital economy as well as overall transatlantic commerce.40

Hate speech, fake news, and consumer protection. Both the United States and Europe are challenged by online hate speech, illegal content, and digital fraud, yet each side of the Atlantic has different laws and tools to tackle these challenges.

Many EU countries, for instance, have specific laws that criminalize certain types of speech, whereas the First Amendment to the U.S. Constitution guaranteeing free speech has been interpreted by U.S. courts in ways that permit a broader range of speech, although also with some narrow exceptions. As a result, U.S. platforms have come under fire in a number of European countries for alleged failures to remove such content promptly from their sites. Germany has been the most vociferous critic, and has presented a draft law that would fine social networks up to €50 million for failing to remove slanderous or threatening online postings.

In May 2016 a number of U.S. companies agreed with the European Commission on a code of conduct that committed them to review and remove illegal hate speech from their
There is also growing concern on both sides of the Atlantic about fake news being circulated on social media platforms. In December 2016 Facebook began rolling out new tools in the United States to prevent the spread of misinformation, working with a number of fact-checking partners. In January 2017 the company announced it would start filtering fake news for users in Germany. The German government, however, has charged that some companies have been less effective than others.

In addition, the European Commission in March 2017 launched an initiative to ensure that social media platforms’ terms of services are brought into conformity with European consumer law. The Commission has challenged companies to ensure that EU consumers have judicial redress in their own country, not just before courts in the United States; that consumers have the right to withdraw from online purchases; that terms of service cannot limit social media networks from liability when it comes to performance of services; that sponsored content be identified as such; and that digital scams and fraud be removed from digital sites.

**Intellectual property challenges.** Copyright law has struggled to adapt to the digital world. Content providers are concerned about internet piracy and inadequate compensation by digital service providers. Platform companies, in turn, are concerned that they could be held liable for infringements or illegal conduct of users of their systems, whose actions they do not control, due to unclear or excessively broad legal frameworks.

In the United States, fair-use exceptions for copyright and intermediary liability protection have been key to enabling the growth in platform companies and the digital economy.

In Europe, however, debates rage. The European Commission has presented a legislative package to modernize EU copyright rules, including a new directive on copyright in the Digital Single Market, that could require digital service providers to monitor user-uploaded content and license the use of short digital excerpts from publishers. Some EU member states, such as Germany and Spain, require search engines and news aggregators to pay copyright fees to publishers when they display short excerpts from their articles. In Spain, Google closed the Spanish version of Google in response. In Germany, major publishers decided to waive their rights so they would still be indexed by such search engines.

**Data and Trade**

Digital flows have become the lifeblood of world trade and the global economy. Recent estimates suggest that the potential economic growth to be realized from liberalizing barriers to internet access and digital trade across the G20 could be as much as $4.2 trillion. Realizing this opportunity, however, will depend heavily on removing constraints that inhibit universal internet access and preventing the emergence of new barriers to digital trade.

Some of the most important hurdles to digital commerce are conventional barriers rooted in the analog economy. These include onerous customs procedures and duties. In a recent survey, 44% of European e-commerce businesses reported that logistics and distribution are the most difficult barriers to cross-border digital trade. Basic differences among postal regimes can also confound small- and medium-sized companies engaged in e-commerce. Traditional barriers to services trade are also major impediments to digital commerce. Simplifying and harmonizing such standard regulations could go far to enhance the efficiency of global digital trade.

Beyond these traditional barriers, a range of novel impediments to digital trade have arisen. Those include widely differing approaches to data privacy and protection, data localization requirements, shortcomings in achieving a balanced intellectual property regime for the digital environment, legacy financial services regulations, and increasing instances of online censorship.

Protection of personal data has become a major issue in global trade. Over 100 countries either have in place or are developing personal data protection regulations, many of which differ considerably from country to country.

Some restrictions are designed to protect individual privacy rights or enhance national security. Others are protectionist measures designed to shield domestic services, content and production from outside competition. They may sound appealing to local politicians, but they can serve to limit domestic economies from leveraging the economic and social benefits of data flows and find themselves unable to access cloud services, internet-connected machines, or content produced through online collaborations with trading partners.

The EU and U.S. can play a role in guiding the international community towards harnessing the potential — and navigating the challenges — associated with data flows for economies and for global trade in an inclusive and open manner.
For example, negotiations for a Trade in Services Agreement (TiSA), under way since April 2013, aim to establish global minimum requirements for trade in sectors such as financial, digital and transport services. Participants include the United States, the EU, and 21 other WTO members, who together account for 70% of global trade in services. The TiSA is expected to establish new market access commitments and universal rules that reflect 21st century trade, and agreement between the United States and the EU is likely to be decisive.

Unfortunately, the two sides have failed to unite behind common principles. Since the EU considers data protection to be a non-negotiable fundamental right, not a trade barrier to be used as a bargaining chip in a trade negotiation, the European Commission prefers to deal with countries bilaterally, agreeing to cross-border data transfers only after officials scrutinize the partner country’s privacy laws and determine that they are equivalent to those in place within the EU. This makes it difficult for the EU to negotiate a plurilateral deal like TiSA.

Meanwhile, the EU’s General Data Protection Regulation, set to go into effect in 2018, expands the number of options deemed acceptable by EU authorities when it comes to legitimizing international data transfers, but still maintains that data is prohibited from being transferred outside the EU without approval from an EU supervisory authority.57

The United States and others who want to move ahead with a TiSA provision on free flow of data argue that if the European Commission doesn’t come along, there will be a chill to digital trade with the EU. Similar challenges await the EU in other trade deals it is negotiating.58

The Changing Nature of Work

Perhaps the most significant challenge facing the United States and Europe is the potential impact of the digital economy on jobs and the nature of work. Forecasts vary widely. Some see boundless opportunities in previously unimagined job categories, enhanced productivity and liberation from mundane routines. Others project massive dislocation and unemployment, widening skills gaps and growing income disparities.

Isolating digitization’s particular influence on labor markets is no easy task. The European and North American economies are in a continuous state of flux. Every hour, hundreds and even thousands of jobs appear and disappear for many reasons: technological progress, changing consumer tastes, demographic changes, migration flows, energy and raw materials costs, cyclical fluctuations, government policy changes, uneven productivity performances, and many other powerful factors that shape the competitive clash of companies. Many different factors simultaneously affect the demand for labor, the labor supply, the level and cost of wages across each continent.59

Given the economy’s churn, it is exceedingly difficult to differentiate between job losses or job gains caused by digitization and those caused by these other factors. Each affects the others in many different ways. These factors are tied up with one another in one great knot. Untangling that knot, and pulling out the digitization strand cleanly, is exceedingly difficult. Nevertheless, as digital technologies automate many human tasks, it is clear that the nature of work will change profoundly.60

Debate has been fueled by a variety of studies. In 2013, researchers at Oxford University estimated that around 47% of total U.S. employment had a “high risk of computerisation” by the early 2030s.61 This finding was largely corroborated by McKinsey, which estimated in 2015 that some 45% of U.S. employees’ work time was spent on tasks that could be automated with existing technologies.62

Others aren’t so sure. In 2016 a team of OECD researchers drew on an extensive new OECD data set to review the Oxford University study, and arrived at much lower estimate that only around 10% of jobs were under “high risk of computerisation”.63 They argued that predictions of job automation should focus more on specific tasks related to particular jobs rather than on whole occupations.64

A 2017 study by PriceWaterhouseCoopers, in turn, drawing on previous research, estimates that around 38% of existing U.S. jobs, 35% of German jobs, and 30% of UK jobs could be at potential risk of automation by the early 2030s. They conclude that the most exposed sectors in the UK include wholesale and retail trade, manufacturing, administrative and support services, and transport and storage. They estimate that in the United States, three of the same four sectors are exposed (administrative and support services being the exception), with the finance, accommodation and food service, and information and communications sectors also most exposed than in the UK. In Germany, construction is the most exposed sector, along with transport and storage, manufacturing, and finance and insurance.65

While these studies arrive at different conclusions, each focuses narrowly on the technical feasibility of automation displacing jobs, while a host of additional factors are likely to be equally relevant.
Just because it is technically feasible to replace a human worker with a robot does not necessarily mean that it makes economic sense to do so. The marginal cost of replacing a worker with a robot system in manufacturing, for instance, is approximately $130,000 today, whereas the marginal cost of applying AI software to a radiology or financial services task may be quite low and the productivity gains quite high.66 Autonomous cars raise a host of safety, liability and regulatory concerns that range far beyond pure technical feasibility. Such factors suggest that digitization’s impact on jobs is likely to be quite uneven sector-by-sector and country-by-country, and in many instances over longer time horizons than envisaged by some.67

Projections such as those cited above also tend to ignore the economy’s churn, and in particular the fact that digitization is also creating new jobs, occupations and even sectors of the economy. By bringing supply and demand together in real time, the platform economy is making many markets more efficient, is matching labor to employment needs more effectively, and is enabling workers to better map out their education and career pathways.68 In many industries and countries, the most in-demand occupations or specialties did not exist ten or even five years ago, and the pace of change is set to accelerate. By one popular estimate, 65% of children entering primary school today will ultimately end up working in completely new job types that don’t yet exist.69

Unfortunately, it is much more difficult to quantify the effects of future jobs and professions that today do not even exist. One study estimated that in 2013 around 6% of all UK jobs, and 10% of all London jobs, were of a kind that did not exist in 1990, and that by 2030 at least 5% of UK jobs may be in areas related to new robotics/AI of a kind that do not even exist now. Some studies project that digitization could lead to entirely new employment structures in which some percentage of workers shift between various forms of employment and will at times have multiple, simultaneous workplaces. This is already becoming apparent, as more and more workers exist simultaneously in multiple worker categories. Once again, official statistics have not yet caught up with these changing realities.70

Furthermore, digitization should generate productivity gains that cause additional higher average real income levels and spending that will support additional jobs, particularly in sectors that are less easy to automate, such as healthcare and other personal services, where robots are more likely to complement and enhance, rather than replace workers.71 This digitally-enabled productivity surge has, however, not yet come to pass. In fact, over the past decade productivity growth in advanced economies has slowed significantly. Various explanations have been given for this, for instance, the shift from generally higher-productivity manufacturing economies to lower-productivity services economies; a slower rate through which digital innovations radiate through the economy; that businesses lag in harnessing the full potential of digitization; and that such technological advances boost productivity only after a gestation period.72 Whatever the causes, projections of employment effects become difficult.

**Widening Skills Gaps**

What the debate on digitization’s impact on jobs makes clear, however, is that skills and continuous learning matter more than ever.73 The World Economic Forum estimates that by 2020, more than a third of the desired core skill sets of most occupations will be comprised of skills that are not yet considered crucial to the job today. They also underscore that social skills such as persuasion, emotional intelligence and teaching others will be in higher demand across industries than narrow technical skills, such as programming or equipment operation and control.74 Individuals who are able and disposed to adapt and reskill throughout their working lifetimes are more likely to ride the digital wave than those who are not.75

For all the talk of job losses due to digitization, and despite relatively high unemployment in a number of European countries, especially among the young, the European Commission is concerned that the EU could actually face a shortage of up to 900,000 skilled ICT workers by 2020, due to mismatches between demand and skills. The Commission estimates that around 40% of people in the EU workforce do not have adequate digital skills and that 14% have no digital skills at all.76 Skills gaps are also apparent in the United States, where there were 353,000 open jobs per month in the manufacturing industry through August 2016.77

A related concern is that digitization could accelerate income disparities. Income inequality is greater in the United States than in any other democracy in the developed world, and it is growing in Europe. By eliminating some routine jobs while requiring new skills in others, digitization rewards those who can adapt successfully, while those with less education and skills fall behind. Automation and digital technologies have reduced the need for many production, sales, administrative and clerical jobs, while demand has increased or low-skilled jobs that are harder to automate. The result is what MIT economist David Autor calls a “barbell-shaped” economy with strong demand at the high and low ends and a “hollowing out” of the middle.78 Between 2000 and 2015, the United States created eight million net new full-time equivalent positions; 5.36 million of those were in low-skill interactive work and the remaining 2.64 million in high-skill interactive work.
But during this period, some 2.5 million net medium-skill jobs were lost. McKinsey finds that automation could displace anywhere from 10-15% of middle-skill jobs in the decade ahead.

**Conclusion**

In short, the net long-term effect of digitization on total employment in the United States and Europe could be either positive or negative. Yet digitization has clear implications for skills development, and offers a cautionary note regarding income disparities. Opportunities for lifelong vocational education and training to help people adapt to increased automation is becoming an imperative to success in the digital economy. Workers will need to adapt to changing employment possibilities and be prepared for many jobs during their working life. Yet it is even more important to ensure that labor flexibility does not lead to precarious living standards. Both public and private leaders must address the need for economic security as workers adapt to changing circumstances.
Endnotes


8. Ibid.


12. Ibid.


19. Ibid.

20. For a review of various studies and policy conclusions, see Daniel S. Hamilton, Europe 2020: Competitive or Complacent? (Washington, DC: Center for Transatlantic Relations, 2011), Chapters 2 and 19.


34. The key passage in PPD-28 is that “all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information. U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.”


56. Meltzer, op. cit.


60. Manyika, et. al, op. cit.


68. JManyika, et. al, op. cit;


73. Manyika, et. al, Digital America, op. cit.


79. Manyika, et. al, Digital America, op. cit.

80. Ibid.


