European Cloud Alliance

CLOUD TRENDS TO FOLLOW IN 2018

CYBERSECURITY, DIGITAL TRANSFORMATION AND PRIVACY

@CloudAllianceEu

Cloud Trends to Follow in 2018: Cybersecurity, Digital Transformation and Privacy

Context

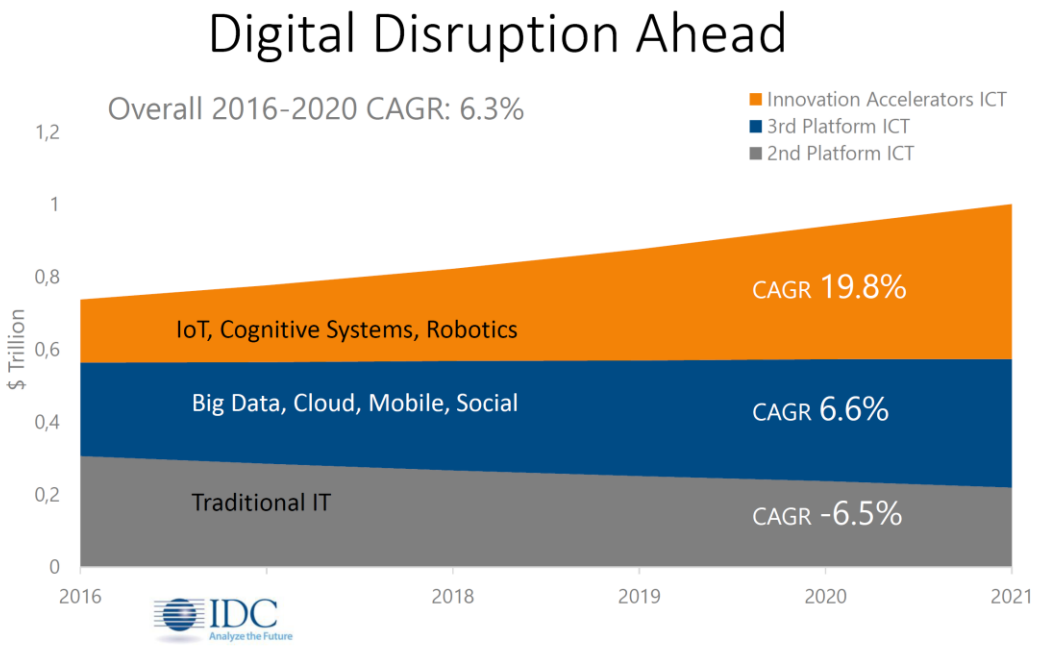
1. Cloud in Europe: A Progress Report

A look forward to 2018

The most confident forecast we can make about 2018 is that the cloud revolution will continue to accelerate, both in Europe and elsewhere.

Although growth in IT spending in Europe has been slow in recent years, growth in cloud services has far outpaced the overall market. According to Forrester Research, IT spending in the EU, after marking time at 1.6% in 2017, is expected to increase to 2.2% in 2018. Forrester attributes the speedup to an improving economy in Europe and the increasing eagerness of European enterprises and governments to seize the benefits of digital transformation. But Forrester also forecasts much more aggressive growth for the cloud in particular. The analyst firm says that cloud-based applications will continue to progress, from 15% of the EU software application market in 2015 to 27% in 2018.

IDC goes further and finds that new technologies such as Big Data, Cloud, Machine Learning and Internet of Things are growing rapidly, while spending on traditional IT is declining. Within just a few years, spending on traditional IT will be a minority share of the market.



At the European Cloud Alliance our mission is to promote the advantages of cloud computing for the European economy. In this article we take a brief tour of likely trends in the 2018 European technology landscape. We have chosen to focus on the business and public policy implications of these trends rather than nitty-gritty technical details. Please don't forget to share with us your agreements and disagreements.

2. Digital Transformation is reshaping the EU economy

Context

The phrase "digital transformation" is to be seen everywhere these days. But what does it mean, exactly? In truth, there is no official dictionary definition. In one common definition, exemplified in the quote from the European Commission's Peter Friess below, the phrase is just an umbrella term that covers a host of technologies, including but not limited to Cloud Computing.

The Digital Transformation and Europe: A View from The EC

"Industry is a pillar of the European economy. The manufacturing sector in the European Union accounts for 2 million enterprises, 33 million jobs and 60% of productivity growth. We stand on the brink of a new industrial revolution, driven by next-generation technologies such as the Internet of Things, Cloud Computing, Big Data and Data Analytics, Robotics and 3D printing. They open up new horizons for industry to become more adventurous, more efficient, and more capable of developing innovative new products and services. Recent studies estimate that the digitization of products and services can add more than 110 billion euros of annual revenue to the European continent in the next five years."

--Peter Friess of the European Commission's DG CONNECT

But we could also define digital transformation as primarily concerned with the remaking of organizational form and function, rather than technology as such. It holds that digital transformation is about using technology to reconstruct enterprises and other organizations from the ground up around new value-creation processes based on information.

Modern digital transformation extends the capture and use of information from the sales transaction to the entire range of activities that organizations perform. Every transaction that an organization engages in can be digitized and subjected to further processing and dissemination: every interaction with a customer, employee, sub-contractor, supply chain partner, patient, student, government official or citizen; every exchange with a non-human store of information, be it a web site, database, household appliance, delivery truck or orbiting satellite—all this and more can be transformed into data and manipulated in the virtual world of computers.

The purpose of this incessant capture and transformation of information is to create value for humans—customers, employees, stakeholders of all kinds—and for society at large. The promise of digital transformation is that it will allow enterprises and other organizations (non-profits, government agencies) to create more value and to create it in new ways, while using resources such as energy, financial capital and human capital more efficiently.

What to expect in 2018

There is a common belief in Brussels and elsewhere that Europe has somehow fallen behind in the digital transformation race. But this idea is highly debatable. It is true that many of the world's largest tech firms have grown up in the United States, thanks in large part to the size of that country's internal market. It is equally true that Chinese Internet firms, who also enjoy a vast internal market, are emerging as the leading challengers to the U.S. giants.

But it is not true that Europe is missing the digital transformation wave. According to Huawei's Global Connectivity Index, which compares national economies based on 40 indicators that track ICT's impact, six of the world's top ten digital economies are in fact European. At the European Cloud Alliance we are confident that 2018 will see rapid strides in the digital transformation of European enterprises of all sizes, supported by cloud service providers.

2017 Ranking of the World's Top 10 Nations on the Global Connectivity Index

RANK		COUNTRY	SCORE
1	-	United States	77
2	-	Singapore	75
3	-	Sweden	73
4	-	Switzerland	69
5	▲ 1	United Kingdom	67
6	▲ 1	Denmark	66
7	▲ 1	Netherlands	64
8	▲ 1	Japan	64
9	▼ 4	South Korea	64
10	-	Norway	62

Privacy

3. Rights of Governments and Citizens

Government and the tech industry are searching for common ground on data access

We begin this preview of 2018 not with technology, but with the rapid evolution of the legal frameworks that determine who can see whose data, and in what circumstances. It is fair to say that Europe stands at the epicenter of these changes, not only because of the GDPR (see the next section), but because the EU is leading the way in establishing new rules for the ways governments can access or regulate the data of private citizens. Among Europe's recent initiatives are the EU-U.S. Privacy Shield (an agreement protecting the privacy rights of EU residents when their data is processed in the U.S.), proposed new e-evidence legislation (setting rules for cross-border access to electronic evidence in criminal and terrorism investigations), and a proposed new regulation on cross-border transfers of non-personal data within the EU.

In the pre-Internet era, virtually all the information that organizations and private individuals owned was stored on their own premises or on the premises of specialized institutions such as banks. When democratic governments sought access to that information for legal or national security reasons, they had to follow established procedures—for example, by using well-understood legal instruments such as subpoenas or search warrants. But now, as more and more business and personal information has moved to the cloud, and the cloud's physical infrastructure becomes global, the rules controlling government access to such information have become less clear.

Today, many Internet privacy advocates, joined by several prominent tech firms, fear that governments—not just authoritarian regimes, but also western democracies—may abuse their power to access information in the cloud. Several key issues are at stake, and all are likely to continue generating controversy in 2018.

What to expect in 2018

A first issue concerns the right of governments pursuing law enforcement investigations to access electronic information stored in other countries. We have mentioned the e-evidence proposal, which only concerns such access between EU member states. But there is also the question of access between Europe and the rest of the world. A prominent recent case involves an effort by U.S. authorities to compel Microsoft to turn over customer data stored in its Irish data center. The tech firm objected that complying with a U.S. warrant in this situation would require it to violate Irish and EU data protection laws. Microsoft won this case in a U.S. Court of Appeals, but it has now gone before the U.S. Supreme Court. At this point no one can be certain what the outcome will be, but Microsoft can be expected to argue its case vigorously. The European Union plans to join the debate by submitting a brief to the Court explaining the EU data protection laws that govern the transfer of personal information outside of the EU.

Cloud providers like Microsoft and Google argue that existing mechanisms for exchanging law enforcement information across borders have been made obsolete by the Internet and must be modernized. According to Microsoft's VP of EU Government Affairs, the solution ultimately cannot

be litigation but "a legal framework—recognized in international law—that creates the basis for governments to access data when they need to." Bills to address the issue have been introduced in the U.S. Congress, but progress is likely to remain slow in 2018.

A second issue is data localization. The digital economy cannot thrive without a free flow of business and technical data across borders, both within the EU and with Europe's trading partners in other parts of the world. Yet EU member states still place many legal restrictions on the movement of data outside their borders because of concerns over what might happen to it once it moves. The GDPR sets out clear rules for the movement of personal data across borders, both within and outside the EU. But it does not cover non-personal data—a category which includes much business and technical data and is extremely important to the digital economy. Consequently, the European Commission (EC) has proposed a new regulation setting forth a detailed framework for the free flow of non-personal data within the EU. It also includes provisions aimed at facilitating the portability of data between providers. This is a welcome development, because industry-led efforts towards more transparency in the market can only be positive, so long as a high degree of consistency with the GDPR framework is ensured. 2018 will therefore witness a spirited debate about the whole proposal!

Another key issue for 2018 concerns encryption. Do Internet users and organizations have an unrestricted right to use unbreakable encryption on their documents and messages? Or do governments have a right to compel tech firms to provide "backdoors" to encryption that would allow law enforcement to read encrypted content under certain conditions? Government officials in the U.S., the UK, France and other democratic countries have often expressed the view that encryption backdoors are necessary for law enforcement and anti-terrorist activities. But many privacy advocates forcefully oppose this idea, and neither the U.S. Congress nor the European Parliament appear ready to pass laws mandating backdoors, although national parliaments in certain EU countries such as France and the UK may be less reticent. Sharp disagreements on this issue are likely to persist in 2018.

4. Complying with the GDPR

Context

The biggest event in the domain of privacy in the world in 2018 will certainly be the arrival of the EU's sweeping new data protection law, the General Data Protection Regulation. After more than five years of discussion and debate, the GDPR will officially enter into force on May 25, 2018. It is a landmark in the history of world privacy legislation, and its impact will be felt far beyond Europe. There are many kinds of sensitive data that require protection in the cloud era, including financial information and intellectual property. But in the eyes of the public and policy makers, the most important kind of data—the kind that most needs protection—is data about individuals. In 2018, thanks to the GDPR, every organization in the world that interacts with Europeans will be obliged to focus its attention on this issue.

The GDPR is a dense legal text consisting of over 50,000 words in 173 recitals and 97 articles. We will not attempt to describe its many important provisions here. A vast literature on that subject already

exists and is readily accessible online.

Perhaps the most important takeaway about the GDPR is that it is much more than a long list of data protection "dos and don'ts". Above all, it embodies the idea that privacy is a fundamental human right, and seeks to develop basic legal principles that apply to the processing of personal information by all organizations, public or private.

If your organization has any relationship whatsoever with EU residents—whether it be as employees, paying customers, free users of your service, suppliers, sub-contractors, or merely random visitors to your web site—then achieving verifiable compliance with the GDPR will be your Legal and Compliance team's most important task during 2018.

What to expect in 2018

Beyond the detailed steps needed to achieve compliance, there are a few very general principles that should guide your effort. The most important is that GDPR compliance is as much or more about changing enterprise culture as about implementing new procedures. The GDPR requires that you think about all personal information your business touches in a fundamentally new way.

The definition of personal information in the GDPR is extremely broad—it can even include something so seemingly impersonal as a photograph of an empty landscape, if that photograph can be linked to an identifiable individual. Consequently, your entire staff and all your partners must understand the new rules. For every piece of personal information that your organization gathers and handles in any way, you must be able to justify why you gathered it, what you are doing with it, and how long you intend to keep it. You must also allow the subject of that information to view it, receive a copy of it, correct any errors, ask that it be erased, and object to or withdraw previously granted consent for certain uses.

While culture is the key, technology also makes a difference. Modern IT applications that have been crafted with the GDPR in mind will make compliance easier. All of the leading cloud providers have pledged to comply with the GDPR and to incorporate features that help their customers comply. Some cloud providers have even developed compliance management tools. These tools automatically inventory instances of GDPR-covered data in your applications, flag compliance gaps, and automate the process of filling them and documenting the solutions used.

However, you must remember that the primary burden for compliance remains with the enterprise. No software package or cloud service by itself can achieve compliance for you, because decisions about what personal data to gather and how to process it are ultimately made by you, not by your providers. Your board and your enterprise leaders must take direct responsibility for ensuring that the necessary changes to organizational culture and mindset occur.

Further reading

Final version of the Regulation, released 6 April 2016

5. Online advertising in the EU maybe be shaken up by ePrivacy

Context

The GDPR is not the only major new European privacy law you need to plan for in 2018. It has a sister law, known as the ePrivacy Regulation, which is if anything more controversial than the GDPR itself. ePrivacy focuses more specifically than GDPR on protecting the privacy of users of online services. As of late 2017 its final form was not yet certain, but its provisions have been the subject of heated disagreements between privacy advocates and the online advertising industry.

The ePrivacy Regulation stands in the same relation to the GDPR as the ePrivacy Directive of 2002 (the so-called "Cookie Directive") does to the 1995 Data Protection Directive. A draft of ePrivacy was approved by the European Parliament in late October 2017 and a final version is expected to be approved sometime in 2018 after "trilogue" negotiations between the Parliament, the Commission, and the Council of Ministers.

The main objection of online advertisers is that ePrivacy in its current form will require strong user consent for the user tracking and profiling, now widely used for targeted advertising. Obtaining such consent, the industry argues, will be difficult in practice for publishers and very inconvenient for users, who will be bombarded by even more "Do you consent to this?" pop-ups than under the current Cookie Directive. The consent requirement may even be impossible to meet for the numerous invisible third parties whose cookies help advertisers target you online, because these third parties have no direct relationship with users. Moreover, electronic communications services are now much more than just a way of sending information from one user to another. They increasingly use new AI-powered tools to transform and enhance that information in ways that users find valuable. By processing users' electronic communications data, cloud service providers can help them manage their agenda, sort their content, automate certain replies, and make targeted recommendations, among other benefits. These are all features that the ePrivacy law in its present form could make difficult or impossible.

Privacy advocates argue, on the other hand, that ePrivacy will finally give users true control over their online experience. They—and not publishers or advertisers—will decide what is done with information about them or about what they do online. If publishers can't obtain user consent for tracking and ad targeting, the advocates say, then they should ask users to pay for content directly instead of financing it indirectly through ads.

The Regulation also endorses end-to-end encryption and, in its present form at least, prohibits so-called "backdoors" that could allow governments to gain access to online communications.

Many observers expect the Council and perhaps also the European Commission to listen with more sympathy to the complaints of the online ad industry. But support for the privacy advocates' view appears quite strong in the Parliament, so it remains unclear how far the pendulum can swing back toward the industry camp. It seems unlikely that the privacy advocates will lose all that they have gained in the initial draft.

What to expect in 2018

As it stands now, the ePrivacy regulation could have a far-reaching impact on digital businesses and on cloud stakeholders in particular. As a provider or as a user, you will need to pay close attention to the ePrivacy debates and begin thinking now about what you will do if significant new restrictions on processing electronic communications data are passed.

Further reading

The new EU ePrivacy Regulation: what you need to know

The flaws of ePrivacy: Will phones still be allowed to be smart?

Cybersecurity

6. Cybersecurity begins at home (with your culture)

Context

The safest prediction about cybersecurity for 2018 is that we will continue to see successful cyberattacks carried out against well-known organizations and individuals. But is there nothing we can do to protect ourselves and our organizations from these seemingly unstoppable attackers?

The reply many experts give to this question, while not exactly reassuring, does offer an alternative to despair: the great majority of cyber attacks begin with simple, easily avoidable human errors committed by well-intentioned employees or users. Therefore, the key to reducing these attacks is not just better technology (although that is of course essential), but above all a better culture, one in which all individuals—including senior executives—take personal responsibility for cybersecurity.

Analysis by Microsoft suggests that 90% of successful cyber attacks probably begin as phishing attacks—that is, deceptive emails that lure users into downloading malware or disclosing their passwords. Once the attackers breach the enterprise's outer perimeter in this manner, they deploy sophisticated techniques to set up a long-term base camp inside the victim's network. From this base the hackers explore information assets accessible on the victim's network, and then exfiltrate the assets they wish to steal.

In addition to users clicking on something they should not click on, there are other common but avoidable errors that open the path to attackers. These include:

- IT system administrators forgetting to set passwords on servers and databases (as has recently happened to a number of inexperienced users of Amazon Web Services)
- IT organizations failing to apply security updates (known as "patches") to software (as happened in the recent attack on Equifax)
- Organizations failing to update obsolete software or hardware (as in the case of the NHS hospitals in Britain whose PCs running older versions of Windows fell prey to the WannaCry ransomware attack)

These examples show that security depends on enterprise culture and the behavior it encourages in individuals. To reduce the risk of a cyberattack, you must take control of the elements in your culture that make you vulnerable. You must warn, train, and cajole your employees to recognize and avoid the actions that open the door to hackers. This is a difficult task that can only be accomplished with sustained effort. But it can be done.

What to expect in 2018

Cybersecurity technology will get better. As we have said above, security culture is more important than security technology. But you cannot ignore technology, because the methods of attackers are constantly improving. If you do not continually upgrade your cyber defenses and your basic computing assets (both hardware and software), your vulnerability will increase as time passes. You can't defend against the attacks of the today or tomorrow with yesterday's technology. Indeed, a key

advantage of cloud services, quite aside from cost and flexibility, is the fact that these providers are obliged to keep their infrastructure constantly up to date, and in so doing they relieve you of that burden.

We cannot review the vast range of new cybersecurity offerings now available. But here are two key principles you should apply when evaluating such technology:

- Does the product or service encourage users to adopt safer behaviors? Good security tools "nudge" users and organizations to do the right thing: for example, warning when too many administrators have broad access privileges or when a user tries to perform a risky or forbidden action (like sending a file with sensitive data to an unauthorized recipient).
- Does the product or service leverage the intelligence of the cloud? Global cloud providers like Microsoft or Google see far more "bad" things on the Internet than any single user organization—no matter how large. The cloud providers are building services that pump the results of their vast cyber intelligence operations directly into your applications and devices. You should take advantage of these services.

2018 will also see major new cybersecurity legislation come into force in EU member states. The EU's Directive on security of network and information systems (NIS Directive) was passed last year, and member states have until May 2018 to transpose this directive into their national laws. The NIS Directive is the first piece of EU legislation specifically devoted to cybersecurity. It is intended both to increase cybersecurity and harmonize the measures adopted by the member states. However, the fact that NIS is a Directive rather than a Regulation means that there could be significant divergences among the different national implementations. The EC has also released an update of its Cybersecurity Strategy, which contains some proposals that could lead to greater harmonization, including an expanded role for the European Union Agency for Network and Information Security (ENISA) and a possible new EU cybersecurity certification framework. However, considerable uncertainty remains about the implementation of these proposals, and the march toward a stronger and more unified European approach to cybersecurity will still be under way in 2018.

Finally, there is a growing concern over the risks of cyber warfare between nation states. Recent years have seen a wave of cyber attacks by nation states against civilian targets in rival nations. Some far-sighted tech leaders have proposed a Digital Geneva Convention to protect civilians from such actions. Building the support needed to make this idea a reality will take a number of years, but awareness of the dangers of unrestricted cyber warfare is certain to grow in 2018.

7. It's time to abolish the password

Context

A new slogan is becoming popular in cybersecurity circles: Identity is the new firewall. We live in a world where business is no longer conducted exclusively within a controlled perimeter of corporate-issued devices. People today expect to work anywhere, on any device, whether approved by IT or not. Consequently, the firewall no longer marks the true perimeter of your enterprise network. When enterprises can no longer isolate themselves from the world behind a wall, identity becomes the new firewall. In such a world, the credentials that determine who has the right to access your information

assets must be protected from compromise at all costs.

Identity is about much more than devices and locations. It enables companies to apply rigorous and granular controls to decide who is allowed to do what based on each user's organizational role, authorized privileges, and verified needs, regardless of how or where the user connects. By focusing on authenticating and managing user access rights, organizations in the post-firewall world can protect their information assets regardless of where it is stored or how it is accessed.

What to expect in 2018

The technology that manages identity in an enterprise setting is very complex and evolving rapidly. There are innumerable products and services on the market and more in the pipeline. But if there is one thing you can do that will make the online identity of your employees and users more secure, it is to move away from the traditional password as the core method for establishing identity. Passwords can be stolen, forgotten or guessed. If they are the only thing standing between hackers and your information assets, you have likely already lost the battle.

How is it possible to abolish the password? One simple technique is to replace traditional passwords—hard to memorize, short but often cryptic strings that include odd characters and numerals—with passphrases, which are longer strings composed of three or four real words that embody some private, easily memorized user secret. The U.S. National Institute of Standards has recently rescinded its long-standing advice to create passwords using odd characters and numerals and to replace them every few months. It now recommends that users create passphrases and says there is no need to change them unless they have been compromised or forgotten.

But there is an even better way to improve passwords, and that is to augment or even replace them altogether them with stronger authentication factors. The idea of multi-factor authentication or MFA is to combine something you know (a password, passphrase, or PIN) with something you have (a specific pre-registered device, such as a PC, smartphone or USB key) and perhaps even something you are (a biometric scan of a finger, face, or iris).

With MFA it is no longer possible for a hacker to steal a user's credentials with a phishing email. Having the user's user name and password is of no use, because logging in also requires having the user's specific device and perhaps even a nearly impossible-to-duplicate biometric feature. To be sure, one can always imagine spy thriller scenarios where the bad guys manage to overcome all the barriers to hacking created by MFA. But it is safe to say the great majority of enterprise users will never face such implausible scenarios.

MFA can be used both for traditional on-premises software and for cloud services. The best way to implement MFA for both kinds of applications is to use a cloud-based directory service that provides identity and authentication services for all users and applications.

If there is one thing you do for your organization's cybersecurity in 2018, it should be to mandate MFA for all of your users.

8. Securing the Internet of Things

Context

When we talk about the risks of cyber attacks, we usually think of hackers hijacking a conventional device such as a PC or server and using it for malicious purposes. There are a billion or so PCs in the world, and several billion smartphones, so there is plenty to worry about. But the world is already on the cusp of a dramatic new wave of growth in connected devices that will see many tens of billions of ordinary "things"—household appliances, cars, factory machinery, elevators, and countless less consequential devices such as light bulbs—transmitting data and receiving instructions over the Internet. A conservative estimate is that this "Internet of Things", or IoT, will consist of 75 billion or more devices by 2025.

These billions of Internet-connected "things" will display new and more intelligent behaviors than their dumb predecessors. They will be more energy efficient, easier to maintain and safer to operate, and will eventually even learn to anticipate our instructions or needs. The IoT will thus transform the invisible technical infrastructure of modern life. In doing so, it promises to make our economies more productive and drive higher standards of living for all.

Yet, given the ease with which hackers have attacked our existing PCs and servers, it is to be feared that they will also seek to turn our many billions of newly connected IoT devices against us. If hackers seize control of these devices, they could command them to disclose private data or sabotage our homes, factories or even cities. Such are the risks we face if we can't figure out how to make the IoT secure.

One problem with the IoT in its current immature state is that most devices do not yet have enough security built in. A refrigerator or elevator is typically less intelligent than a PC, and of course a light bulb is far less so. Often it is too expensive or technically difficult to put enough intelligence in IoT devices to implement adequate security in addition to their primary functions. IoT manufacturers may also lack experience in building enterprise-grade security software. Gartner even predicts that within 5 years " half of all security budgets for IoT will go to fault remediation, recalls and safety failures rather than protection".

An urgent task going forward will be to change this state of affairs and make sure that the IoT is made secure enough to be trusted with the immense power it will acquire over our daily lives.

What to expect in 2018

Today, there is no global standard for IoT security, but several efforts are underway in the world's major standards bodies. This is a fast-moving and very technical area. The IoT is evolving an exceptionally complex ecosystem with many participants, all of which will need to comply with emerging standards and best practices. In 2018 we should expect user organizations and the firms who supply them to start to develop a more mature understanding of where they fit into IoT's brave new world.

One way to look at how security affects this ecosystem is to classify its inhabitants into four basic roles:

- IoT hardware manufacturers or integrators. They must produce devices that are not only designed to be attack-resistant from the outset, but can be securely upgraded throughout their lifetimes (because technology and attack methods always evolve).
- IoT solution developers. These are the teams that write the software applications deployed on IoT hardware. Their key responsibility is to think about security from the start of the development process and to avoid known pitfalls (such as using hard-coded passwords or incorporating third party software components with known vulnerabilities).
- IoT solution deployers. These are integrators who set up devices, connect them, and install software. Deployment is a critical moment in the lifecycle of an IoT solution. A compromised authentication key or an improperly set password can create a lurking vulnerability that may later be exploited by opportunistic attackers.
- IoT solution operators. These teams will manage deployed IoT solutions throughout their lifecycles, and will be responsible for monitoring security status, pushing upgrades, and responding to incidents.

Keeping the IoT secure will require careful coordination among these many players. The EU Network and Information Security Agency is working with chip suppliers to develop baseline IoT security requirements. It is also expected that ENISA will be given a mandate to develop "Trusted IoT" labels as part of the EU's proposed cybersecurity certification scheme.

The IoT will still be a very young technology in 2018, but expect government agencies and standard bodies to make significant progress toward defining effective standards and best practices.

Further reading

Cybersecurity Policy for the Internet of Things

Artificial Intelligence and Big Data

9. The machine learning revolution is just beginning

Context

In the mid-1950s, the still obscure academic field now known as Computer Science spawned an even more obscure sub-branch that came to be known as Artificial Intelligence. Over the next 60 years or so AI gave rise to countless works of science fiction and some interesting theorizing. It attracted many brilliant researchers and generous government funding. But it failed to yield major practical breakthroughs in such important areas as machine translation, speech recognition or image classification. The one clear finding of AI research was that genuine human intelligence and purely logical reasoning are two very different things.

But over the last few years, things have changed abruptly. A new branch of Artificial Intelligence called "deep learning", based on sophisticated mathematical methods of pattern recognition, has risen to prominence. The new approach has led to remarkable breakthroughs in precisely the areas where traditional AI failed to deliver—machine translation, speech recognition, speech generation, and image classification. The discoveries have revolutionized almost overnight the cloud-based consumer services we are all familiar with. Promising work in many other areas, such as self-driving cars and medical diagnosis, is also advancing rapidly.

The terminology of this new field makes it sound more mysterious than it really is. The "deep" in deep learning does not refer to "deep thinking" or anything similar. It merely says that these methods process data by applying successive transformations stacked up in layers. Deep learning models are also sometimes referred to as Neural Nets, because early ideas in the field were loosely inspired by analogies with the human brain. But today most researchers in the area no longer think their work says much about how the brain works.

Deep learning builds on earlier work in the broader field of machine learning, which uses probability and other analytical methods to learn things from data. The key idea is that we want to build models that can learn how to perform certain desired tasks (machine translation, face recognition, etc.) without needing to be taught a lot of complicated rules painstakingly crafted by humans. It turns out that creating by hand all the rules that would be needed to perform such tasks is exhausting, and we humans probably aren't smart enough to do it. Instead, with deep learning, the models train themselves to do the job by looking at vast numbers of examples and methodically correcting their mistakes until their output becomes acceptable.

What to expect in 2018

Although academic researchers in deep learning continue to publish new ideas at a frenetic rate, many of the biggest advances now come from industry. Google, Facebook, Microsoft, Amazon, Baidu and many other firms, including dozens of startups, now compete to hire the brightest PhDs. Nor is all of the path-breaking work concentrated in Silicon Valley. World-class deep learning labs are at work in China, Canada, Britain and other countries.

Perhaps the most remarkable thing about the current deep learning boom is how accessible this approach is to newcomers and innovators. There are three key ingredients for building a useful deep learning application: software tools, computer power, and data. Let us briefly review each of these ingredients. The first has become essentially free, the second is rapidly dropping in price, and the third—although not always easy to obtain in sufficient quantity—can be found nearly everywhere in our hyper-connected economy, including in Europe.

Deep Learning software. The world's biggest tech firms are now locked in a battle to give away the most powerful deep learning software tools their developers can devise. Google's TensorFlow, Facebook's PyTorch, Microsoft's Cognitive Toolkit, Amazon's MXNet—all are available for free under open source licenses that let users build anything they can imagine. These tools make the work of designing and training powerful deep learning models much easier and faster. They also hide most of the complicated math at the heart of deep learning algorithms. These tools are still rapidly evolving and adding new features, and in 2018 they will only get better and more useful.

Of course one might well ask why the tech giants are in such a rush to give away this valuable intellectual property, the very tools they use internally to build their own commercial products. Surely there is a catch? The answer is two-fold. To be sure, most of these firms hope that developers who use their tools will deploy applications on the firms' own cloud services, which of course are not free. But another motive is the intense competition to attract the best and brightest minds in computer science from all over the world. The firms reason that if the smartest graduate students and developers learn to use their tools, they will be more likely to want to work for the firms that created them.

Computer power. Getting a deep learning model to perform tasks like speech recognition or image classification with reasonable performance doesn't require a supercomputer. Once they have been trained, many of these models can now be deployed effectively on smartphones. But the training itself is another matter. If it is to be done in a reasonable amount of time (hours and days rather than weeks and months), it requires high performance processors that can perform vast numbers of calculations in parallel. Researchers have discovered that the GPUs (graphics processing units) originally designed for computer video games perform quite well at training deep learning models. The chips are expensive, but prices are coming down. You can buy or build PCs that can pack in multiple GPUs. You can even use gaming laptops to train deep learning models. But while such devices may be useful for developing algorithms, in large scale production applications of machine learning users are increasingly turning to the cloud. All the leading cloud providers now rent high-end GPU machines for deep learning by the hour or even minute. Moreover, providers like Google and Microsoft are deploying their own specialized deep learning chips whose performance surpasses that of standard GPUs. Expect prices for all these cloud-based machine learning services to keep declining in 2018.

Data and Intellectual Property. By far the most important ingredient in a successful deep learning application is data. In the current state of the art, a machine translation service such as Google Translate or Bing Translate needs to see millions of sentences from the languages it is intended to translate before it can perform effectively. To train such a service, its creators must obtain vast collections of identical documents rendered in different languages. These collections are known as corpora (singular: corpus). One of the most famous examples of a large corpus that has actually been

used to train most of the world' leading machine translation services is the Digital Corpus of the European Parliament, which contains nearly 1.4 billion documents in 23 languages created by the Parliament's army of human translators.

Of course, not every enterprise can or should undertake the development of its own machine translation service. The task is immense, and it would be challenging to surpass the existing efforts of Google or Microsoft. But there are countless other deep learning applications waiting to be developed. Since the software development tools and the necessary compute power (cloud-based) are affordable and readily available, it all comes down to that third critical ingredient, data. Many European enterprises own or have access to unique data sets that can be used to train deep learning applications. We expect that 2018 will see a wave of such applications developed by European firms and deployed in products and markets all over the world. Some of these breakthroughs will come from Europe's established giants in the automobile, aviation and equipment industries. But many others will come from SMBs and startups.

The growing value of data in the age of machine learning has not escaped the notice of European owners of large collections of data to which they hold copyright, nor of the EU policy makers responsible for fashioning a modernized copyright law that reflects digital realities. The EC's proposed Directive on Copyright in the Digital Single Market has given rise to a sharp debate between copyright holders and those who want the freedom to apply mining algorithms to published data without fear of violating copyright law. One of the provisions of the Directive is the so-called Text and Data Mining Exception, which would grant a mandatory exception to copyright rules for certain groups that wish to conduct such data mining. However, the scope of the exception and the definition of exactly which groups would be covered by it is controversial. Should it apply only to scientific researchers? Or should journalists and perhaps even market researcher also be included?

This debate will certainly rage on in 2018. It is not in the interest of Europe or its digital economy to restrict access to published data by machine learning innovators, whoever they might be. The risk to Europe is that, faced with such restrictions, European entrepreneurs will simply move elsewhere.

But copyrighted data is not the only kind of intellectual property whose importance is amplified by the cloud revolution. Patents—especially the many thousands of patents used by the closed and open source software running in cloud applications—play a large if often overlooked role in the cloud market.

A cloud application is a complex assembly of many pieces of software from different providers—operating system, system utilities, middleware, database, networking, security and identity management, and the application itself and its various components, which may be numerous. What happens if one of these pieces in your cloud application infringes—or is claimed to infringe—a patent owned by some other company? What happens if that patent owner decides to sue you, the user, even though you did not create the bundle of software components used by your cloud application? You don't want to be forced to hire lawyers to defend yourself from cases like this. Ideally, you want your cloud providers to assume the risk on your behalf and provide some kind of guarantee that you will be insulated from such disruptions. Fortunately, some of the leading cloud providers are aware of this concern and have taken measures to address the issue. Since they own many thousands of patents themselves, they are in a strong position to reduce the intellectual property risk faced by cloud users.

10. Who really controls Europe's data?

Context

The European Union appears to be on a collision course with the American consumer Internet giants Facebook, Google and Twitter. That at least is a widely held view, often expressed in media reporting. The stated issues of contention turn mainly around user privacy and, to a lesser but still significant extent, the rights of content publishers. Many observers also believe that Europe wishes to curb the disproportionate influence held by the American giants in European markets. However, European regulatory institutions such as the EC and member-state Data Protection Authorities are bound by legislation and administrative rule-making. They do not act on whim.

What to expect in 2018

The most obviously relevant piece of legislation here of course is the GDPR. Simply put, the GDPR and the forthcoming ePrivacy Regulation (both discussed in a previous section) are going to require some fundamental changes in the business practices of almost all participants—not just the American giants—in the targeted online advertising industry. While it is too early to predict exactly how or when these changes happen, we should expect major developments in this area during 2018.

GDPR and ePrivacy requirements that users must consent to use of their data may help level the playing field for European marketers and publishers. Such requirements will reduce the value of third party data for ad targeting purposes, because such data will not come with user consent. The result could be a decline in the power of intermediaries like Facebook and Google, making first-hand customer information gathered directly by European marketers and publishers (with users' consent) more important.

The underlying question in the debate about the influence of the Internet ad giants really boils down to: who should control Europe's data? While political and media attention has been concentrated on the well-known consumer Internet firms, this focus obscures a more important fact: to a large extent, the most valuable data sets concerning European customers and markets have not yet been exploited. These are the data sets that European firms—manufacturers, retailers, service providers—gather directly in their operations or their interactions with customers. According to an IDC study commissioned by the EC, the value of data-related products and services in the EU may exceed 100 billion euros by 2020 if all goes well.

The great promise of machine learning for the European economy is still in the future. Every European enterprise should be looking in 2018 for data derived from its own activities that can be fed into deep learning and similar algorithms.

In short, the answer to the question "who controls Europe's data" is that, to a large extent, you do.