GENEVA INTERNET PLATFORM
digwatch

NEWSLETTER

Issue 59 - Friday, 30th April 2021

In AI we trust?

The EU's newly proposed AI regulation takes a risk-based approach. Here's what companies, users, policymakers – and the EU – need to know.

Pages 2, 10

DATA BREACHES

As the data of millions of Facebook and LinkedIn users ends up in the wrong hands, we take a look at the issues regulators face.

Pages 2, 6

SOLARWINDS

The SolarWinds attack, which affected at least nine US federal agencies and several countries, was officially attributed to Russia by the US authorities. What happens next is critical.

Page 3

SEMICONDUCTORS

The ubiquitousness of chips means that the current shortage carries significant geopolitical implications for the USA, Europe, China, and Taiwan.

Pages 8-9

UPCOMING GLOBAL EVENTS

Our calendar helps digital policy practitioners keep track of the main global conferences and meetings. Take a look at May's events.

Page 12

The top 3 trends in April: Regulating AI, data scraping, and the aftermath of SolarWinds

Each month we analyse hundreds of unfolding developments to identify key trends and underlying issues which impact the work of policy practitioners working in these fields. Here's what mattered in April.

1. Regulating AI

The EU's proposed regulation could become a global standard, but there's a long journey – and some tough decisions – ahead

Governments' interest in regulating AI systems is now more manifest than ever, especially after the EU's long-awaited draft proposal published on 21 April. The proposal takes a risk-based regulatory approach: If a system poses exceptional risk, it will be banned; if it's considered high-risk, it will be heavily regulated; if the risk is limited, it's then a matter of being transparent about it. *Read more on page 10.*

Experts say there's a striking similarity with the GDPR: Both take a long-hand approach, meaning that the proposed rules regulate anyone – anywhere – whose system is used within the EU or affects EU citizens. This normative approach and jurisdictional reach could help the proposal become a global gold standard for AI regulation and the development of AI systems.

But the EU needs more than a claim to a global standard. It will have to assess the potential impact of the new legal framework, or risk losing out (again) to the USA and China: Tight regulation is likely to discourage the private sector from innovating and developing AI systems in the EU; but a laxer approach would simply delay finding solutions to important issues, including deeply ethical ones, maybe until it's too late. Experts dealing with antitrust issues around the globe know this all too well.

Essentially, European policymakers and politicians will need to agree on how far and deep the regulation should go. They will need to decide on which systems are too risky for society, which can be tolerated (albeit regulated) in the interest of innovation, and which to let off the hook. These decisions will ultimately impact the level of trust which society will have in AI systems and those who run them – not just in the EU, but around the world.

2. Data scraping

Facebook and LinkedIn's latest breaches were a data scraping incident, and not a hack... there's more to this than just technical lingo

We're quite accustomed to learning about massive data breaches. Facebook believes this activity happens – and will continue to happen – regularly.

What stood out this month, however, is that both Facebook and LinkedIn responded to the massive data breaches – affecting 500+ million users on each platform – in a similar way. According to the social media giants, it wasn't a hack, but rather a data scraping incident from years ago, with the databases of personal information being posted online only now.

At face value, both terms – hacking and scraping – conjure elements of technical mischief. However, both may lead to the same dire consequences: Personal data that is meant to be private or protected is now in the public domain, and can be exploited by bad actors. Breach or no breach, users are at risk of falling victim to phishing or other fraudulent practices, as has already been the case. Both are an unwelcome invitation for more criminal activity, which is broadly regulated and punishable by law around the globe.

However, this reveals deeper societal issues, and is a reflection of the price we're willing to pay for more free services, social connections, innovative products, and convenience. Ultimately, whether we want to – or how we go about – holding companies to higher standards is a reflection of the value we attach to our personal data and privacy, and that of future generations.

We take a deep dive at what data scraping means for regulators and users on pages 6-7.

3. The aftermath of SolarWinds

The espionage was carefully planned and executed – what happens next is even more critical

The USA has formally attributed last year's SolarWinds attack to the Russian Foreign Intelligence Service (SVR). At least nine US federal agencies were breached and several other countries affected.

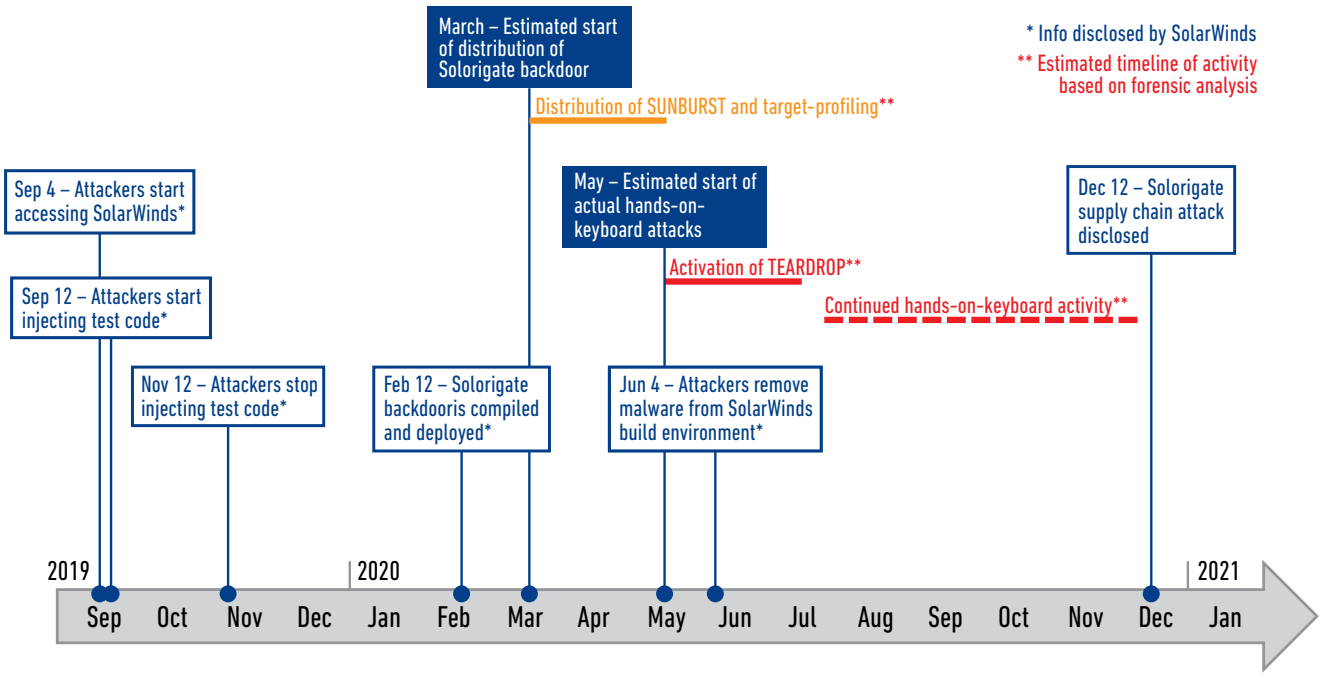
What followed since this attribution is tit-for-tat: In an executive order, US President Joe Biden sanctioned around 40 Russian individuals and companies, after which Russia expelled 10 US diplomats. NATO, the EU, the UK, and Australia immediately expressed support in favour of the USA – an indication that the Biden administration worked closely with its allies to amplify the message and show a united front.

What happens next will be much more critical. Although the attack was labelled as espionage (meaning information was taken, but nothing was destroyed or disrupted), it doesn't mean that the perpetrators won't use their newly acquired intelligence for a cyberattack. Plus, it's still unclear to the USA whether it has managed to wipe its breached systems clean from the intrusion.

The main question is whether the sanctions will be enough to dissuade Russia (and others) from carrying out similar hostile activities, and whether the USA will change its deterrence and 'defend forward' strategies. The White House has already signalled that the sanctions were only a part of the steps the USA would be taking, and that 'there will be elements of our responses to these actions that will remain unseen.'

The USA will need to weigh the implications of its responses, and make sure it does not cross the threshold of what's considered an armed attack. While deterrence may be ineffective, experts have suggested that the USA should focus more on beefing up its defences.

On a more positive note, experts also say both sides have left the door open for dialogue: Biden said it was now time for tensions to de-escalate through dialogue and diplomacy; Russia did not shoot down Biden's idea for a summit. Time will tell.



The timeline of the SolarWinds attack (Credit: Microsoft)

The digital policy developments that made headlines in April

The digital policy landscape changes on a daily basis. Our aim is to save practitioners time: We decode, contextualise, and analyse ongoing developments, offering a bite-sized authoritative update. There's more detail in each update on the *GIP Digital Watch* observatory.


same relevance

Global IG architecture

G7 digital and technology ministers outlined plans to cooperate on a wide range of issues, including supply chains, digital standards, data flows, and Internet safety.

The 2020–2021 Group of Governmental Experts on lethal autonomous weapons systems concluded its work.

The call for session proposals for the 16th Internet Governance Forum meeting is open until 26 May.


low relevance

Sustainable development

Egypt launched the Decent Life project to connect 1300 villages to optical fibre.

Bangladesh, Brazil, China, Egypt, India, Indonesia, Mexico, Nigeria, and Pakistan initiated the digital learning initiative E9.

The Economic Commission for Africa established the Learning Girls in ICT Initiative.


increasing relevance

Security

The USA formally attributed the SolarWinds cyberattack to Russia and imposed sanctions. *Read the commentary on page 3.*

The European Parliament adopted a regulation requiring online platforms to remove or disable access to terrorist content within one hour of notification.

Several EU institutions were affected by an IT security incident. Apple supplier Quanta Computer Inc. was hit by a ransomware attack.


increasing relevance

E-commerce and the internet economy

China's competition authority fined Alibaba US$2.8 billion over anticompetitive practices. Russia's competition authority launched investigations into Yandex and YouTube. A report by Australia's antitrust regulator argues that measures are needed to address the market dominance of Apple and Google's app stores.

Google was fined more than US$36 million in Turkey for abusing its dominant position in search engine services.

The USA proposed a global minimum tax for companies, including the tech sector. The Organisation for Economic Co-operation and Development (OECD) reaffirmed plans to reach a global solution for taxing the digital economy by July 2021.

US cryptocurrency exchange Coinbase joined the stock market.

The central banks in the UK and Japan launched exploratory work into digital currencies.


same relevance

Infrastructure

At an online summit on semiconductor and supply chain resilience, US President Joe Biden reiterated plans to strengthen the country's semiconductor industry and secure its supply chain.

The USA added seven Chinese supercomputing entities to the export control list.

Digital rights

The data of 533 million Facebook users was leaked to an online hacking forum. Additionally, the data of 500 million LinkedIn users was posted for sale. *Read our analysis on pages 2, 6–7.*

TikTok was sued in the UK over the processing of children's data. Consumer and child protection organisations asked Facebook to cancel plans to create an Instagram for children.

Content policy

Facebook expanded the scope of its Oversight Board to also decide in cases in which the company chose not to take down content. The Board postponed its decision on Trump's ban from Facebook and Instagram.

Livestream platform Twitch announced it would ban users for severe misconduct that occurs outside of the platform.

Twitter was criticised for acting upon a request from the Indian government to remove tweets seen as critical of the government's handling of the COVID-19 pandemic.

Instagram released new features to address hate speech. Twitter launched an initiative to analyse the harmful impact of its algorithms.

Jurisdictional and legal issues

The US Supreme Court issued its opinion in the Google LL.C v. Oracle America InC. case, ruling that copying a portion of the Java SE computer program by Google is protected as 'fair use'.

A high court in Pakistan lifted the TikTok ban imposed by the country's telecom regulator. A Russian court fined Twitter for not removing content encouraging minors to take part in unauthorised protests.

An Amsterdam court ordered Uber to reintegrate five drivers excluded from the platform through an automated process.

New technologies (IoT, AI, etc.)

The European Commission launched a draft regulation for AI systems. *Read more on page 10.* The US Federal Trade Commission warned it would take action against discriminatory AI systems.

Brazil adopted an AI strategy. Canada outlined plans for updating its AI strategy and launching a natiaonal quantum strategy. Finland established the Quantum Institute.

The UK outlined plans to regulate the cybersecurity of internet of things devices.

Data scraping and the problems regulators and users face

On 3 April, Business Insider revealed that a database containing the personal data of 553 million Facebook users was uploaded to a hacking forum. A few days later, an archive with the personal information of 500 million LinkedIn users was also posted for sale.

What's the difference between data scraping, a data breach, and a data leak?

Data scraping is an automatic extraction of large amounts of data from websites, databases, or apps. In web scraping, a program 'crawls' through content on a website or platform and lifts, or copies, publicly available information automatically and creates a document (excel sheet, accounting ledger, website) for scrapers' use. It is a common practice in business; for instance, this is what search engines do to provide us with the information we're searching for. It's also how price comparison websites work, such as those comparing air ticket prices or insurance costs.

Data scraping is not unlawful, but it needs to follow certain rules – such as requiring people's consent to scrape, and a legal reason to use data scraping. The problems arising out of data scraping are related to how the data is scraped (with or without consent), what it was used for (data analysis or posting on hackers website), and who shoulders responsibility for any risks and threats.

A **data breach** is when a computer system or data is unlawfully accessed or weakened by malicious actors without the knowledge or authorisation of the owner, leading to exposure of confidential, sensitive, or protected information. Data breaches (or hacks) are unlawful. In many cases, they are considered a crime.

A **data leak** is when private data (or a private database, even if made up of various pieces of publicly available data) is made available to the public. A data leak does not require an active breach into the computer system. It usually is a result of poor data security practices or accidental human error. The responsibility for data leaks is tied to the obligation to keep data secure and to undertake necessary measures to do so.

Facebook and LinkedIn's immediate response was similar: The breaches were large-scale scraping incidents, rather than hacks. This drew the attention of data protection regulators and users around the world.

Facebook said the incident happened in August 2019, when malicious actors used a vulnerability in the 'How people can find me' feature, which was later fixed. It later emerged that the data was scraped on several occasions from 2018 to 2019 (we'll get to the issue of timelines further down). In LinkedIn's case, it is unclear how old this information is and whether it was aggregated solely from the platform.

Here are at least five main issues which regulators must resolve.

Issue #1: How platforms classify personal data as private or public

Both companies said the data was public. In Facebook's case, the company added that it's the users' responsibility to make sure 'their settings align with what they want to be sharing publicly'. In other words, if a user chooses certain settings on the platform, Facebook takes this as the consent which certain data protection regulations require. The problem here is that Facebook is not properly explaining to the users the full extent of the consequences of certain settings for users to make an informed decision.

Plus, if we look at the dedicated resource page, the platform says that public information refers to 'some of the information you give us when you fill out your profile…' or that 'your Public Profile includes your name, gender, username…' The fact that Facebook talks in terms of 'some' or 'including' leaves users in the dark. As a result, users could be providing personal data to Facebook under the mistaken idea that Facebook will keep it private, and hence more secure.

Issue #2: The platforms' responsibility for the personal data they hold, public or not

In some jurisdictions, platforms are indeed responsible for personal data, even if it's already out there and visible to others. For instance, the EU's GDPR says that companies need to have certain technical measures in place to ensure that personal data is processed safely, securely, and according to law.

One can therefore argue that if the data was lifted off the platforms – whether through a vulnerability in the system or by failing to detect scraping activity – then the platforms have a degree of responsibility.

The Irish data protection authority, for one, is arguing along these lines. Digital Rights Ireland, a digital rights advocacy group, is also gearing up to file a mass lawsuit against Facebook on behalf of users who want to be compensated for having their personal data exposed, in breach of the platform's terms and conditions. In the USA, the incident could be considered a violation of Facebook's US$5 billion privacy settlement with the Federal Trade Commission (FTC) to resolve the Cambridge Analytica data scandal, among others. Other user lawsuits are expected to hit Facebook in India and in other countries.

Issue #3: The platforms' attempt to normalise recurrent incidents

Facebook has downplayed the incident not only to shrug off liability, but to normalise this as a chronic occurrence. Facebook is telling users and regulators that the world needs to get used to such incidents and that it does not intend to notify affected users every time this happens.

This insight comes from internal emails that were circulated: 'We expect more scraping incidents and think it's important to both frame this as a broad industry issue and normalise the fact that this activity happens regularly.'

Issue #4: The platforms' obligation to report a data leak

The two platforms did not disclose or notify users or authorities of these incidents at the time. In countries like EU member states and Brazil, which have comprehensive data protection regulations, Facebook and LinkedIn face steep fines for failure to disclose and notify breaches and violations of data protection regulations.

Under the GDPR, and similarly under its Brazilian counterpart the LGPD, scraping of personal data requires consent and a lawful basis. Both the Irish Data Protection Commissioner and the Brazilian Protection and Consumer Defence Foundation of the State of São Paulo – plus others worldwide – are investigating Facebook's practices. Similar steps are being taken in the LinkedIn incident, with the Italian data protection agency opening a probe. The crucial issue for the regulators is to establish, in legal terms, how these breaches fall under the type of incidents that would trigger the platforms' responsibility to report them.

Here is where the timeline comes in: The date when the breach (or leak) took place has a direct impact on the platforms' responsibility. In Europe, for instance, reporting a breach became a legal obligation when the GDPR came into effect in May 2018.

In the USA, Facebook is to some extent shielded from liability for any breaches occurring before June 2019, as part of the Facebook/Cambridge Analytica settlement, except in the state of California, where the Consumer Privacy Act came into effect mid-2018. Yet, the regulators will still need to evaluate the compound data sets and identify timing of the data they include, to then determine when the platforms learned about the scraping incidents, and what responsibilities Facebook and LinkedIn were under at those times.

Issue #5: Users need more awareness of and protection from the risks of exposed personal data

Personal data in the public domain can be used to harm people. Whether the responsibility is the users' (when sharing personal details on social media without understanding, or bothering to understand, the implications), or the platforms' (for not doing enough to protect people's data), bad actors will exploit it.

In these two cases, for instance, the value of the leaks is in the ability to associate mobile numbers and other personal data with an individual. Fraudsters who call someone on a mobile phone will sound more genuine and legitimate if they also know the date of birth, hometown, and place of work. One would think only the authorities and their bank hold such information, right?

The companies themselves, being victims of malicious actors who exploited vulnerabilities on their platforms, will be expected to file legal action, as they have done in the past. But this should also serve as a wake-up call for users. As a consumer watchdog put it: 'People are going to be a lot more skeptical and a lot more careful about providing this whole trove of information to social media platforms.'

The world needs more chips: What this means for the big players

A global shortage: How did we come to this?

Semiconductors – or chips – are at the core of virtually every electronic device. In turn, the production of chips relies on a very complex global supply chain. Producing a single computer chip can involve over 1 000 steps and 70 separate border crossings.

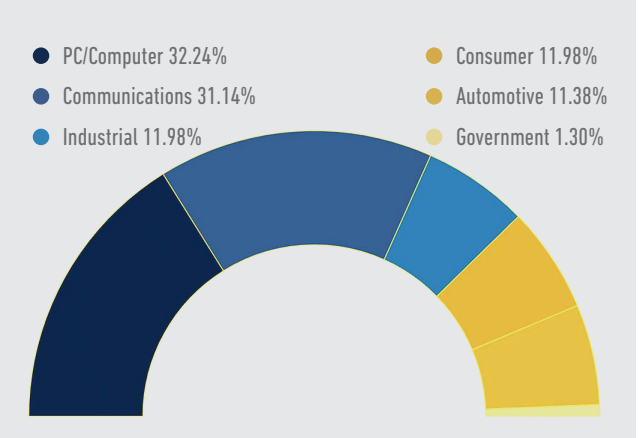
It involves mining and processing the raw materials (such as silicon and boron), designing the chip, and developing the manufacturing equipment. All of this needs to happen before the tiny chip is actually manufactured and assembled into products.

The USA dominates the architecture and design components of the supply chain. US companies, with Intel in the lead, account for almost 50% of the world's chip sales. But more than 80% of the global chip manufacturing happens in Asia, with Taiwan Semiconductor Manufacturing Company (TSMC) and Samsung taking the lead.

Right now, there's a global shortage of chips, which is affecting companies, and indirectly, consumers. Samsung, a chipmaker itself, warned about a 'serious imbalance in the supply and demand of chips in the IT sector globally'.

Apple reportedly had to postpone the production of some laptops and tablets due to the tight supply of chip and display components. Sony has been facing difficulties in supplying its new PlayStation 5. The shortage is expected to last until 2022 or 2023.

One of the reasons is that chip manufacturers – and that's basically TSMC, Samsung and, to a lesser extent, Intel – are sensitive to spikes in demand. The

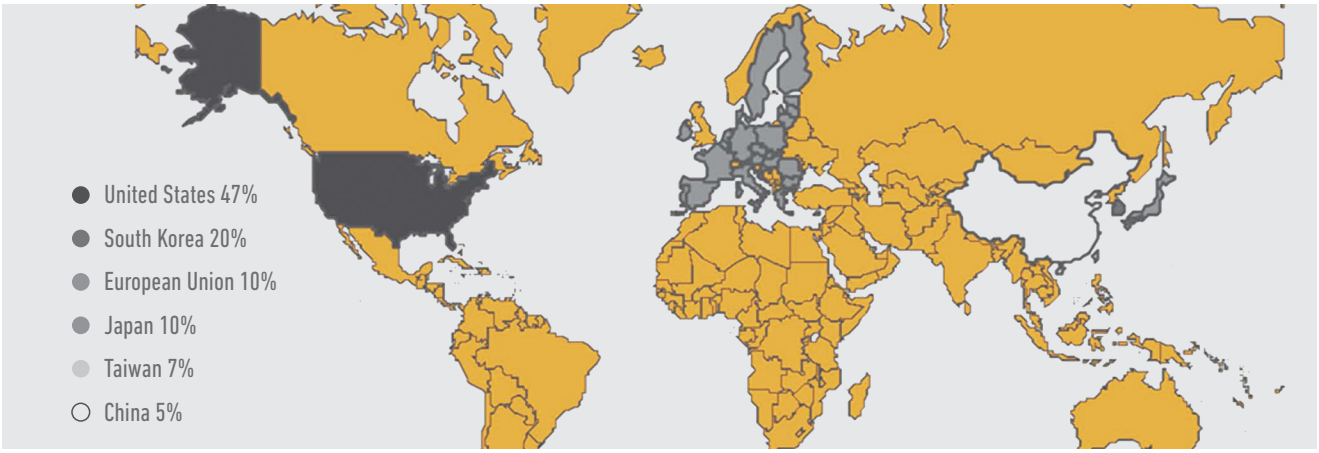


Global microchip consumers. Source: Semiconductor Industry Association

pandemic generated a higher-than-usual demand for smartphones, laptops, and other similar devices, prompting producers to increase their demand. The demand is also coming from other industries, such as carmakers and producers of internet of things devices.

The handful or so companies producing chips have found it difficult to meet this demand. As digital devices become more and more sophisticated, so do chip designs. In turn, this has increased costs for chip manufacturers, which creates a barrier for new players wanting to enter the market. The result is a highly concentrated market in which only a handful of companies can afford to compete and respond to the global demand.

The geopolitical tensions, including export controls and licencing policies imposed by the US government on Chinese companies in recent years, have not helped. For instance, US and foreign firms are now barred from using US intellectual property and



Global market share in 2020. Source: Semiconductor Industry Association

technology to produce chips for Huawei (including Huawei's own designed Kirin chips).

Before these sanctions took effect, Huawei was forced to stockpile chips, and reports argue that large producers such as TSMC prioritised Huawei's orders to the detriment of other clients, affecting the supply chain with long-term effects. Chinese chip-maker Semiconductor Manufacturing International Corporation (SMIC) can only acquire American technology if its suppliers receive a license from the US government.

Natural disasters and incidents are also affecting the production and supply of chips. Chip factories have had to close down or reduce production. Among them were factories in Texas (closed down in February 2021 due to power failures caused by low temperatures); in Japan (after a fire broke out in March 2021); and in Taiwan (due to the ongoing drought).

Geopolitics: How the world's main players have reacted

China and the USA, which have for long competed in the technological sector, have big ambitions. They both want to become self-reliant in the chip market. This would ensure that their home-grown tech industries do not depend on external, possibly unstable, global supply mechanisms.

It is estimated that a country requires a minimum of US$1 trillion up front to achieve a self-sufficient local supply chain; such an investment, in turn, would result in a 35–65% increase in chip prices. That's steep.

China has, for the past few years, been a net importer of chips. Only 30% of its chips have been manufactured domestically. The trade sanctions and export controls imposed by the USA and their effects on Chinese companies like Huawei and SMIC have fuelled China's ambitions for becoming self-reliant.

As a result, China is investing heavily in its own chip manufacturing capabilities, as part of its multibillion-dollar five-year plan. Released in March 2021, the plan envisions considerable support for the local semiconductor industry.

The USA is also not producing enough chips on its own, making its large tech industry heavily dependent on Asian manufacturers. During April's chip summit, President Joe Biden pledged to strengthen the country's semiconductor industry.

Biden also called on Congress to establish a US$50 billion fund for semiconductor manufacturing and research, in line with the draft CHIPS for America Act being debated in the Congress (H.R. 7178/ S. 3933).

There are expectations that a portion of such a fund would go to support the development of advanced chip plants in the USA by TSMC, Samsung, and Intel.

If complete chip self-reliance is almost an impossible task, the next best thing is to source chips from elsewhere. Both China and the USA are now relying on Taiwan's TSMC, which has so far managed to navigate the geopolitical complexities between the two countries by making itself indispensable to both.

Unsurprisingly, TSMC is now facing increased pressure to pick a side between access to the world largest chip market in the USA and the fastest growing one in China.

The chip shortage and complex supply chain also offers an opportunity for new tech partnerships. The EU, for instance, has interesting options ahead, as it tries to achieve its goal to produce one-fifth of advanced chips globally by 2030.

On the one hand, it could join forces with the USA to counterbalance the regional concentration of chip production in Asia. On the other, it could also partner with TSMC and/or Samsung to build or expand factories in Europe. Of course, the bloc could also choose to invest more in European players.

Another potential partnership is between the USA, Japan, Korea, and India (known as the Quad), which have recently agreed to create a Critical and Emerging Technologies Working Group. Among the Quad's aims is to cooperate on diversifying critical technology supply chains.

The adage 'if you can't beat them, join them' couldn't be more true.

The EU's proposed rules for regulating AI systems: The good, the bad, and the ugly

AI is all around us, from our search engines to the smart devices we're using in our homes. The industry continues to push the boundaries of what AI systems can do. New and improved systems make our lives more comfortable, our decisions easier to make, and our surroundings safer.

This all sounds blissful... until it's not. The EU thinks there should be cut-off lines depending on the level of risk to people or infrastructure. Beyond these lines, AI systems should be outright banned (or heavily regulated). Here's the risk-based approach the new European Commission proposal takes:

- **Systems that pose an enormous risk will be considered outright unacceptable.** The cases are listed specifically in the regulation, and include types of facial recognition, and algorithms used to manipulate how we think or what we do.
- **Systems that pose a high-risk will be heavily scrutinised.** These include critical infrastructure which could prove risky to people's lives, and some of the safety components in products (think robot-assisted surgery). The regulation includes both a predefined list of cases and a set of criteria to determine how other systems could be classified as high-risk. If a system is deemed high-risk, it needs to be assessed before being put on the market, and then registered. There's actually a host of other obligations involved, and of course, penalties for not observing them.
- **Systems that pose a limited risk will carry only minor obligations.** Among these are chatbots: The rules will require that we're at least made aware we're talking with a machine.
- **Systems that pose minimal risk can be developed and used freely.** Essentially, that's anything else not falling under the three above. Most of the AI systems currently in use fall under this category.

The next step is for the European Parliament and member states to consider the proposal. It sounds straightforward, but this will actually take years of readings, amendments, and lobbying before the regulations are adopted.

Proposal gets mixed reactions

The proposed rules have been criticised for their vague and broad language, and for not going far enough. They're also riddled with loopholes, especially when it comes to facial recognition technologies and their oft-times discriminatory practices.

For instance, systems that identify people through real-time biometrics are generally banned. Yet, there are some exceptions that apply to law enforcement, which critics believe can be abused.

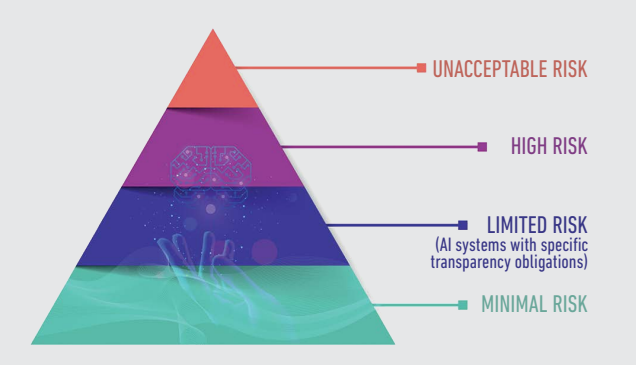
Plus, the ban does not apply to other public entities or companies. Who knows whether they are already using real-time biometrics? Activists say they are, in fact.

Real-time biometrics may be banned, but systems that work on pre-captured images are not. These can still be used to identify people according to race, gender, and sexuality, so although they may well be heavily regulated, companies could still get a green light to use them.

And then, there's the issue of balancing innovation and regulation. Companies think there are too many compliance obligations in place. This argument will not hold enough water for Margrethe Vestager, the European Commission's executive vice-president, who is adamant that Europe 'can only reap the full benefits of AI's societal and economic potential if we trust we can mitigate the associated risks'.

However, it gets more complex when companies say the law will slow down the development of advanced AI systems in the EU. Although big companies may find it difficult – but not impossible – smaller companies or start-ups could be discouraged altogether.

The Commission certainly wants Europe to trust the development of AI systems, but it also wants to encourage a home-grown industry. As we said in our commentary (page 2), the EU will be walking a tightrope, and will have some tough calls to make.



Policy updates from International Geneva

Many policy discussions take place in Geneva every month. In this space, we update you with all that's been happening in April. For other event reports, visit the Past Events section on the *GIP Digital Watch* observatory.

Protection of Critical Water-related Infrastructure (Part II) 13 April 2021

This event, organised by the Permanent Missions of Slovenia and Israel to Geneva, the World Meteorological Organization (WMO), and Microsoft, was a follow-up to the November 2020 roundtable. This second part explored how some of the lessons that emerged from the roundtable could be applied in developing countries, especially in the African region. The event focused on national experiences, and the frameworks and standards that have been put in place, such as the Malabo Convention.

Promoting Circular Economy and Sustainable Use of Natural Resources in the UNECE Region 20–21 April 2021

The United Nations Economic Commission on Europe (UNECE) focused its 69th session on the circular economy and the use of natural resources in achieving the SDGs. One of the roundtables dealt with circular energy, mobility, and digital transformation, and the corresponding new policies and industry best practices. While energy is aspiring to be low carbon or carbon negative, there's also a major push for e-mobility (electric-powered vehicles) in cities and for long-distance transport. Technology is at the core of the fourth industrial revolution, which is embracing all aspects of life and work. The digital transformation has significant bearing on how natural resources are used, moving away from past linear models to new sustainable, service-focused, and circular economy business models.

Digital Economy: Trade and Finance Tour 28 April 2021

The roundtable discussion, organised by the GIP as part of the series 12 Tours to Navigate Digital Geneva, debated the ongoing e-commerce discussions taking place at the World Trade Organization (WTO), with close attention having been paid to the Joint Statement Initiative (JSI) and regional trade agreements. The speakers also looked at the impacts of the COVID-19 pandemic on e-commerce and the role that the latter can play in the post-pandemic world.

What to watch for: Global digital policy events in May

Let's look ahead at the global digital policy calendar. Here's will take place next month around the globe, with direct links to official event websites and programmes. For even more events, visit the Events section on the *Digital Watch* observatory.

May

5-7 May, Science, Technology and Innovation (STI) Forum 2021 (online)

The 6th STI Forum will be held under the theme 'Science, technology and innovation for a sustainable and resilient COVID-19 recovery, and effective pathways of inclusive action towards the Sustainable Development Goals.' The forum will talk about cooperation in STI, a needs and gaps analysis, how to harness technologies for the SDGs, and the impacts of rapid technological change on the SDGs in light of the COVID-19 pandemic. *We'll publish reports from selected sessions.*

17-20 May, RSA Conference 2021 (online)

Under the theme 'Resilience', RSA 2021 will host educational hands-on sessions, as well as traditional speaker-led sessions and keynotes. The topics on this year's agenda include analytics, intelligence and response, policy governance, anti-fraud, hackers and threats, identity, machine learning and AI, open source tools, and privacy.

17-21 May, WSIS Forum 2021 Final Week (online)

The WSIS Forum 2021, which has been ongoing since January, will culminate with a final week dedicated to interactive high-level dialogues, prizes and awards ceremonies, a ministerial roundtable, and the WSIS Action Line facilitation meetings. *As usual, we'll publish session reports from this final week.*

24-29 May, Final Substantive Session of the sixth UN GGE (online)

The sixth UN GGE is about to conclude its work. The group was mandated to study existing and potential threats in the sphere of information security, and possible cooperative measures to address them. It was also tasked with studying how international law applies to the use of ICTs by states, as well as looking at norms, rules, and principles of responsible behaviour of states, and the necessary confidence-building measures. *We'll publish updates on our dedicated space.*

25-28 May, 13th International Conference on Cyber Conflict (CyCon 2021) (Tallinn, Estonia)

Hosted by the NATO Cooperative Cyber Defence Centre of Excellence, CyCon 2021's central theme is 'Going Viral'. Participants will discuss the implications of human crises – such as the COVID-19 pandemic – for cybersecurity and cyberspace.

31 May-11 June, School on Internet Governance, Digital Policies and Innovation (SIDI) (online)

The second edition of the SDI is aimed at graduate students and professionals – primarily from the South Eastern Europe and neighbouring region (SEE+) – keen to learn more about digital innovation, the impacts of the internet and other digital technologies on society and the economy, and the multiple dimensions of digital policy and internet governance. Diplo, the operator of the GIP, is an official SIDI partner.

June

About this issue

Issue 59 of the *Digital Watch* newsletter, published on 5 May 2021 by the Geneva Internet Platform and DiploFoundation | Contributors: Katarina Anđjelković, Stephanie Borg Psaila (editor), Andrijana Gavrilović, Tereza Horejsova, Pavlina Ittelson, Marco Lotti, Virginia (Ginger) Paque, Nataša Perućica, and Sorina Teleanu | Design: Viktor Mijatović, Aleksandar Nedeljkov, and Mina Mudrić, Diplo's CreativeLab. Get in touch: digitalwatch@diplomacy.edu

On the cover

In AI we trust? Credit: Vladimir Veljasević

The Geneva Internet Platform is an initiative of:

GENEVA INTERNET PLATFORM digwatch

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

REPUBLIQUE ET CANTON DE GENEVE

DiPLO www.diplomacy.edu