GENEVA INTERNET PLATFORM
digwatch
NEWSLETTER

Issue 62 – September 2021

Taliban's e-rise

CHILD SAFETY

Apple's plans to keep children safe from online abuse are already on hold. Are the new measures too high a price?

Page 2

ANTITRUST

Governments continue to hit Big Tech with lawsuits. Our new database rounds them up.

Pages 6–7

PRIVACY

China is making a push for privacy. We compare China's new privacy law with Europe's GDPR (spoiler: they're very similar).

Pages 8–9

GIG ECONOMY

In California, the controversial Proposition 22 was declared unconstitutional. There are a few lessons to be had.

Page 10

Ongoing issues in digital policy: Taliban on social media, protecting kids online, and the latest surveillance scandal

1. How to deal with the Taliban on social media

Afghanistan has descended into chaos after the Taliban's takeover of Kabul. The once internet-averse militant group is now tech-savvy, and is using social media as a tool for control. Facebook and others have been shutting down accounts operated by the Taliban or maintained on their behalf. Twitter is monitoring messages for violence.

But social media companies face at least three major dilemmas. The first is how to deal with the channels once used by Afghanistan's elected government, which may now fall entirely in the Taliban's hands. Closing down these channels would mean silencing what remains of the legitimate government, while not intervening would mean allowing the Taliban to take control and fuel these accounts with propaganda content.

The second is how to stop a militant group from spewing propaganda, even if it's content which does not cross the threshold of violence. On social media, the Taliban are broadcasting an airbrushed version of what is happening in Afghanistan for people worldwide to see.

For instance, the Taliban shared photos and videos of militia leaders posing with a known dissident who appeared unrestrained and at ease to demonstrate their civil treatment of opponents. This sits in stark contrast with what news agencies are reporting, including scenes of violence against citizens, and the deadly terrorist attacks in retaliation to American forces who were still in the country.

The third is how to protect Afghan citizens from being targeted for what they say on social media. The fear of retribution is very high – to the extent that Afghans have been racing to delete content that may draw attention from the Taliban. Facebook has been helping Afghan users lock their accounts. For Afghan activists and human rights defenders, being able to remain anonymous will become a matter of life and death.

What Facebook and Twitter decide to do next could determine how other social media companies react. Perhaps it's time to join forces, and consider taking a common approach. The Taliban doesn't yet have a foothold beyond Facebook and Twitter, but it's only a matter of time before they close in on other mainstream social media.

2. Apple announces new measures to protect kids – but why are they on hold already?

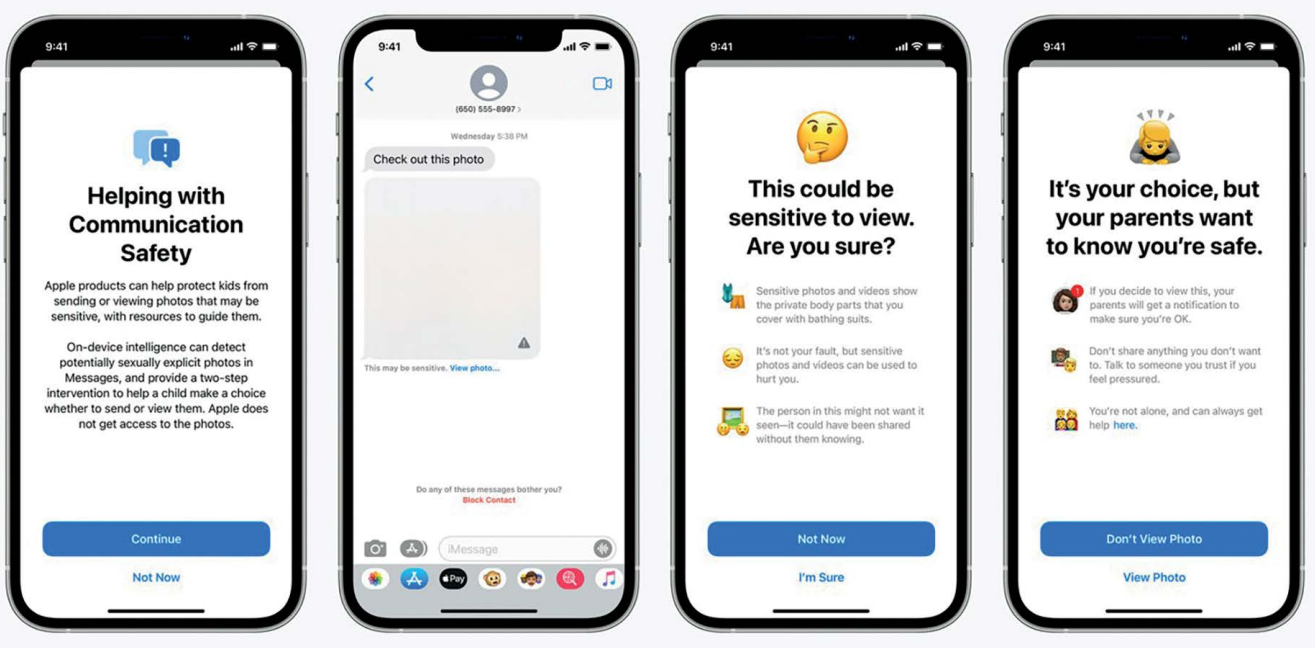
The spread of child sexual abuse material (CSAM) has plagued the internet for decades. While new material appears every now and then, existing photos and videos keep re-appearing, mostly on the dark web.

Apple's new measures for scanning images for CSAM, announced in August, involve two main sets of tools: The first is to detect CSAM on iCloud Photos, and the second is a set of safety features built into the Messages app (read our explainer of the tools). Both involve the scanning of images on users' devices.

The initial plan was to roll out these measures in the USA by the end of the year, but on 3 September, Apple posted an update: 'Based on feedback from customers, advocacy groups, researchers, and others, we have decided to take additional time over the coming months to collect input and make improvements before releasing these critically important child safety features.'

In response to the new measures, more than 90 policy organisations signed an open letter to Apple and warned of at least two main issues. The first is that Apple's ability to scan iCloud Photos is a privacy breach in itself and could 'bypass end-to-end encryption, thus introducing a backdoor that undermines privacy for all Apple users'. The second is that Apple could be strong-armed by governments to use the tool for their own undemocratic purposes, such as identifying other types of content from people's phones.

Apple's response – which explains how the tool was designed with privacy in mind, and does not provide information to Apple about any photos other than those that match known CSAM images – did not manage to assuage the concerns. A 'backdoor is still a backdoor', privacy group EFF explained. In simple terms, 'Apple is planning to build a backdoor into its data storage system and its messaging system… At the end of the day, even a thoroughly documented,



Messages warning children when receiving or sending sexually explicit photos. Source: Apple

carefully thought-out, and narrowly-scoped backdoor is still a backdoor.'

The debate on encryption will not be an easy one. Apple has since promised to revisit the measures and make improvements. If the company manages to do so without creating a backdoor, it will be a win for everyone, including users and human rights defenders. Yet, it's unlikely that the measures will be as effective without some form of reduced encryption.

Ultimately, there's a price to pay to ensure that children are protected. As things stand, the choice will come at a high price for overall user privacy, and the revised measures will likely still come at some cost. So the question is, is it a price worth paying?

3. Pegasus: The latest surveillance scandal

Surveillance is nothing new. Man has always been fascinated with the idea of seeing but not being seen. What recent developments are showing, however, is the growing privatisation of surveillance, in which businesses make money off spyware products.

In July, a database of persons believed to have been potential targets by operators of the spyware tool Pegasus was leaked to Forbidden Stories, a French-based media organisation. French President Emmanuel Macron was on the list, among others.

Pegasus has actually been in use since 2015. Sold by Israeli company NSO Group, the tool exploits a vulnerability in mobile phone software and is able to penetrate devices without requiring the phone user to click on any links to activate it.

The growing trend of profiting from surveillance magnifies the issue of who is responsible. Is it software companies whose products carry vulnerabilities, or users who keep using vulnerable devices? Is it governments, who purchase such tools to hunt down criminals, but may misuse the tools to spy on journalists, religious figures, and academics? Or is it businesses like NSO Group, who, in reality, are not breaking any laws?

This also reminds us of one of the major problems: Existing legal frameworks are too flimsy, and that there's no solid legal basis on which to build a case. An urgent solution, therefore, is to introduce or strengthen legislation that makes it illegal to exploit vulnerabilities, especially for commercial purposes.

Governments are realising how important this is: The 2021 report of the Group of Government Experts recommended that legal frameworks be put in place 'to protect against the misuse of ICT vulnerabilities'.

Until then, targeted people are at the mercy of businesses, governments, and software companies alike.

Digital policy developments that made headlines

***The digital policy landscape changes daily, so here are all the main developments from July and August. We've decoded them into bite-sized authoritative updates. There's more detail in each update on the Digital Watch* observatory.**

increasing relevance

Global IG architecture

The USA and Russia kicked off cyber talks. G20 digital ministers agreed on actions to accelerate digital transition.

A call for nominations for the IGF's 2022 Multistakeholder Advisory Group is ongoing.

same relevance

Sustainable development

Several UN departments have launched a Strategy for the Digital Transformation of UN Peacekeeping. The UN Security Council called for harnessing digital technologies to protect peacekeepers and civilians.

increasing relevance

Security

The USA, EU, NATO, and others accused China of carrying out the Microsoft Server cyberattack earlier this year.

US President Joe Biden has urged the private sector to step up their efforts on cybersecurity, as a ransomware attack on software company Kaseya affected customers in more than ten countries.

Russia proposed a draft treaty on cybercrime, and a new National Security Strategy.

Apple's new child safety measures sparked controversy over privacy, freedom of expression, and encryption. *Refer to our analysis in the Trends section.*

increasing relevance

E-commerce and the internet economy

G20 finance ministers endorsed the OECD agreement on global tax rules.

A California court ruled that Proposition 22, which allows companies to classify their workers as independent contractors, is unconstitutional.

The French competition authority fined Google €500 million over failure to negotiate in good faith with press publishers. A group of 36 US states and the District of Columbia sued Google over app store practices.

US President Biden issued an executive order on competition, tackling net neutrality, antitrust, and data collection. China outlined plans for more regulation in the tech sector.

same relevance

Infrastructure

The US Senate adopted an infrastructure package directing US$65 billion to expand broadband connectivity.

Google plans to build two submarine cable systems connecting the Middle East with southern Europe and Asia.

China revealed plans for the massive deployment of Internet Protocol version 6 (IPv6).

A legal battle between Afrinic and a Seychelles-based company over the use of IP numbers outside of Africa risks hampering AFRINIC's operations.

increasing relevance

Digital rights

Over 50,000 people were potential targets of Pegasus surveillance malware. UN human rights experts called on states to ban the sale of surveillance technology.

The UN Human Rights Council adopted two resolutions on human rights and digital technologies: The first tasks the OHCHR with studying global internet shutdowns, while the second calls for an expert debate on standard-setting processes for new technologies.

China passed its Personal Information Protection Law. *Read our analysis in the Legal section.*

Amazon was fined €746 million in Luxembourg over GDPR violations.

---

increasing relevance

Content policy

Social media companies face challenges in responding to the presence of Taliban-related content on their platforms. *Read our analysis in the Trends section.*

Former US President Donald Trump sued Facebook, Twitter, and Google over alleged censorship.

A Russian court fined Google for not removing content deemed illegal. A Pakistan court revoked a TikTok ban.

---

low relevance

Jurisdictional and legal issues

The Austrian Supreme Court asks the Court of Justice of the EU (CJEU) to review the legality of Facebook's data use of all EU users.

The CJEU Advocate General argued that article 17 of the EU copyright directive is compatible with freedom of expression.

---

same relevance

New technologies (IoT, AI, etc.)

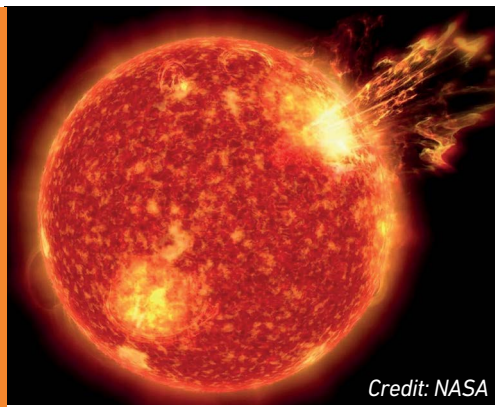
UNESCO member states agreed on a draft set of guidelines on AI ethics. Ireland and Turkey launched national AI strategies. South Africa and Australia recognise that AI-created inventions can be patented.

China's Supreme Court issued rules to regulate the use of facial recognition technology by the private sector. The country's Cyberspace Administration also proposed regulations concerning recommendation algorithms. *Read our In Focus section for analysis.*

#ICYMI

Undersea cables could go offline for months, a new study warns

Catastrophic weather may happen not only on earth, but even in space. When this happens (approximately, every century), the magnetism from a full-blown solar storm could affect undersea cables, leading to an internet blackout, according to new research presented at the SIGCOMM 2021 data communication conference. 'Our infrastructure is not prepared for a large-scale solar event,' the research concluded.



Credit: NASA

Big Tech: To trust or anti-trust

There are two main weapons in governments' arsenal to curb the power of Big Tech: lawsuits and legislation. Both have been increasingly exercised in recent months.

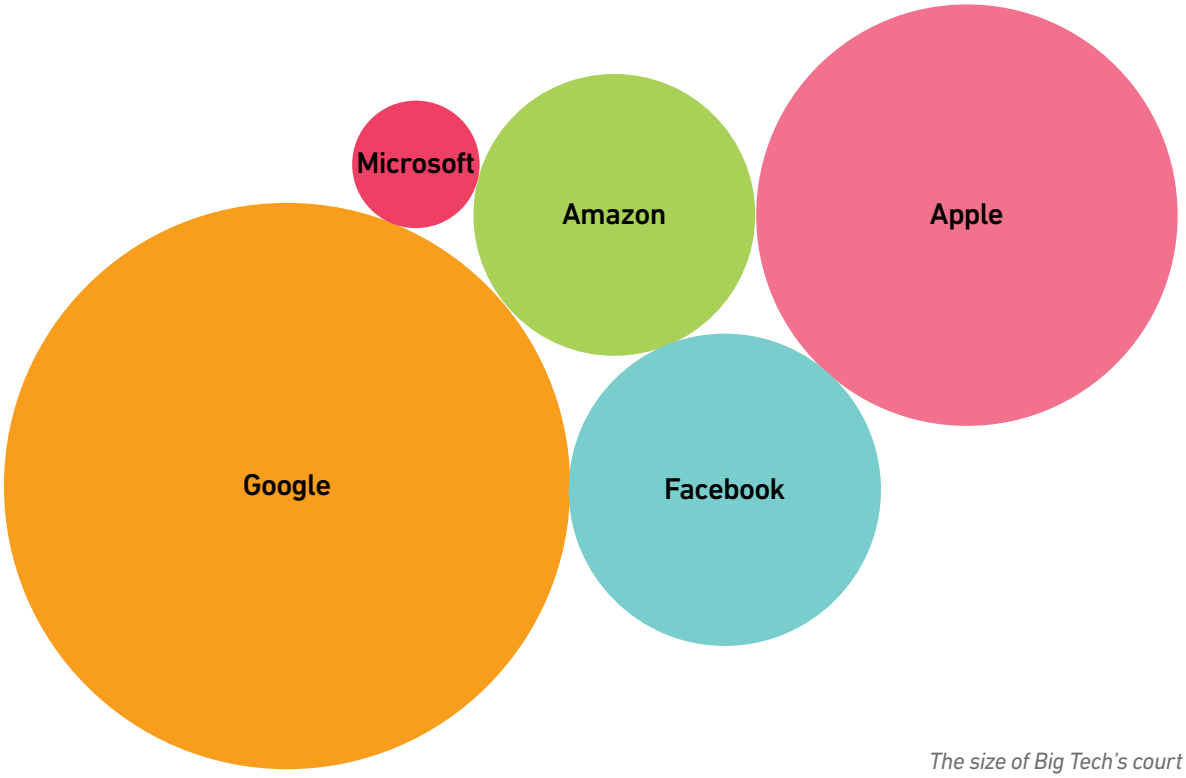
This year will go down in history for many things. In digital policy, it's the spike in the number of investigations and lawsuits launched against Big Tech, and specifically, Google, Apple, Facebook, and Amazon (known as GAFA). These cases come at a point when the companies' revenues are larger than the GDP of entire groups of countries put together.

Our new interactive database of antitrust cases around the world confirms the sheer number of new cases this year, and the fact that the concentration of cases are in the USA and in Europe (and that's mostly Brussels, home to the European Commission). Yet, there are also clear signs that the antitrust battle is expanding to other countries, with antitrust investigations launched in Australia, India, Israel, Russia, and Turkey.

Governments' main concerns were captured very clearly (we won't say succinctly) in last year's report by the US House Judiciary's Antitrust Subcommittee. GAFA control access to the markets in which they operate: for Google it's the general online search and search advertising; for Apple, it's the mobile operating systems; for Facebook, it's social networking; and for Amazon it's online retail. To boot, they try to stay on top (and expand their market power) by monitoring other businesses to identify potential rivals, and by buying out, copying, or cutting off their competitive threats.

GAFA's CEOs may well have different but shared opinions on how many jobs they create, and how much they contribute to the economy, but US legislators had one clear message: 'The result is less innovation, fewer choices for consumers, and a weakened democracy.' It's a sentiment echoing across courtrooms and legislatures around the world.

And yet, even if governments succeed in reigning in GAFA's power, critics are already finding it hard to believe that a new generation of GAFA won't rise again, especially when it comes to the growing markets such as in gaming and augmented reality.



The size of Big Tech's court woes

Changes in the way Apple and Google operate their app markets will enable gaming incumbents (such as the Fortnite creator, Epic Games) to reach swathes of users directly, without having to go through the gates of the App Store or Play Store. These changes are now imminent.

Ongoing efforts to curb the power of GAFA, therefore, must have broad and long-term considerations about what new powers may emerge in the future. Lawsuits and legislation must make sure that history doesn't repeat itself.

Country/re..	Initiator of ..	Against	Type of case	About	Year initiat..	Year decide..	Status		
							Closed	Decided	Ongoing
Australia	Epic Games	Google	Lawsuit	Epic Games sued Google f..	2021	Pending			✓
China	State Admi..	Alibaba	Investigation	At the end of the 100-day ..	2020	2021		✓	
European Union	Amazon	European C..	Lawsuit	Amazon has filed a lawsui..	2021	Pending			✓
	Epic Games	Apple	Investigation	"The complaint, filed	2021	Pending			✓
	European Commission	Amazon	Antitrust case no 40153	The so-called 'most-favou..	2015	2017		✓	
			Antitrust case no 40462	EC is investigating wheth..	2019	Pending			✓
		Apple	Antitrust case no 40437	EC is investigating Spotif..	2019	Pending			✓
			Antitrust case no 40452	EC is investigating Apple'..	2020	Pending			✓
			Antitrust case no 40652	EC is investigating an e-b..	2020	Pending			✓
			Antitrust case no 40716	EC is investigating compl..	2020	Pending			✓
		Facebook	Investigation	The European Commissio..	2021	Pending			✓
		Google	Antitrust case no 39740	The case was on unfair ad..	2010	2017		✓	
			Antitrust case no 40099	The case alleged that Goo..	2015	2018		✓	
			Antitrust case no 40411	Google was investigated f..	2016	2019		✓	
			Investigation	The European Commissio..	2021	Pending			✓
				The investigation is	2021	Pending			✓
France	Ministère d..	Google	Investigation	The French competition a..	2019	2021		✓	

Our database of global antitrust cases clearly shows a concentration of cases in the USA and Europe. View the interactive version.

China's new privacy law: A comparison with GDPR

China has introduced a new privacy law: The Personal Information Protection Law (PIPL). We asked: How similar – or different – is it from the EU's General Data Protection Regulation, often described as a global standard in data protection?

China's PIPL was passed on 20 August by the Standing Committee of the 13th National People's Congress, and will come into effect on 1 November.

Our analysis confirms that on paper, the two are similar, with the PIPL imposing a slightly heavier maximum penalty. There will be more to say when the PIPL is in force, but for now, here's our comparison.

		EU's GDPR	China's PIPL*
How the laws are organised in chapters and titles	≈	The way they are organised is strikingly similar. They both start off with general provisions (Ch.1) and data protection principles (Ch.2). These are then followed by: • Users' rights (Ch. 3 in GDPR, Ch.4 in PIPL) • Cross-border transfers of data (Ch.5 in GDPR, Ch.3 in PIPL) • Obligations of the entities processing data (Ch.4 in GDPR, Ch.5 in PIPL) • Roles and responsibilities of authorities (Ch.6 and 7 in GDPR, Ch.6 in PIPL) • Remedies and penalties (Ch.8 in GDPR, Ch.7 in PIPL) • Specific circumstances (Ch.9 in GDPR, Ch.2 §3 in PIPL) The GDPR has extra provisions (in Ch.10 and 11) related to how the law operates in the EU and the GDPR's relationship with other/former privacy laws.	
The law's reach	≈	They both extend beyond their geographical borders, to protect EU and Chinese citizens, respectively, wherever they are.	
What 'personal data' means	≈	They both have very similar definitions of personal data.	
What 'sensitive personal data' means	≈	These are a bit different. Under the GDPR, this includes: • Biometric identification data • Genetic data • Health data • Political opinions • Racial or ethnic origins • Religious or philosophical beliefs • Sex life or sexual orientation • Trade union membership	Under the PIPL, although the list is similar in a few cases, it includes (and leaves out) quite a few other types of sensitive data. The PIPL's list includes: • Biometric identification data • Financial accounts • Health data • Information on individuals' whereabouts • Minors' (under-14) personal data • Religious beliefs • Specially-designated status
What is considered as a lawful basis for entities to be able to process personal data, and how a user's consent is to be sought	≈	Both laws require that users' consent for processing, and both say that users' consent must be informed, given freely, and can be withdrawn. When it comes to the non-consent basis, both require similar contexts to exist for entities to be able to process personal data (with one exception): • Whenever a contract is involved • Whenever legal obligations so require • Whenever there's the need to protect users' vital interests • Whenever the public interest is involved.	
	≈	The GDPR says that entities can also process data based on 'legitimate interests', a vague term which gives entities more flexibility. An example is for an entity to gather data in order to prevent fraudulent activities.	The PIPL does not include legitimate interests as a valid basis for processing personal data. Instead, it includes 'other circumstances according to law', implying cases in which a legal obligation is imposed on entities.

		EU's GDPR	China's PIPL*
Users' rights	≈	Both provide users with more or less the same set of rights, including the right to information, to have access to and to correct personal data held by entities, and to have their data deleted.	
The entities processing data (which we refer to as entities, or sometimes companies)	≈	Under the GDPR, there are two broad categories of data handlers: • Controller: those who decide which personal data should be collected and how it should be processed • Processors: those who hold or process personal data. (It could well be one and the same individual or entity carrying out both functions).	Under the PIPL, thvere are also two categories: • The personal information processing entity, which is more or less equivalent to the GDPR's controller • The entrusted party, which is the GDPR's equivalent of the processor.
	≈	Other than the terminology, however, the basic rights and responsibilities of those who handle the data are similar.	
Cross-border transfer of personal data, and transfers in specific situations	≈	Both laws allow cross-border transfers of personal data if certain conditions are met. For example, the two laws permit transfers based on contractual agreements formulated by EU and Chinese authorities, respectively, or on any other international bilateral agreement. It is still unclear whether the PIPL mechanisms will be similar to those enabled by the GDPR – such as standard contractual clauses – which are quite comprehensive (and complex). Until there's a clearer mechanism which explains how China will authorise transfers in practice, we can say that both follow the same spirit of allowing transfers only if they are comfortable that their citizens' personal data will be well-protected once it leaves their borders.	
	≈	The GDPR provides for a few derogations when the conditions we described above cannot be met. In essence, the GDPR provides as many avenues as possible to allow the transfer of personal data (as long as there are adequate safeguards to protect citizens).	The PIPL, on the other hand, foresees a situation where personal data will need to be stored domestically. If an entity operates a critical information infrastructure, or processes a large amount of personal data – exceeding the threshold set by the Cyberspace Administration of China – they cannot transfer data. The only exception is if the entity passes the Cyberspace Administration's security assessment, but this suggests that the government will play a major role in deciding what can leave the country.
Penalties	≈	The GDPR imposes a maximum penalty of 4% of a company's annual global revenue	The PIPL imposes a maximum penalty of 5% of a company's annual revenue. It's unclear whether revenue is national or global in this case. If it's a company's global revenue, then the PIPL carries a heavier penalty.

**Note: We've used Stanford's translation as the English version of the PIPL.*

A win for Californian gig workers: Proposition 22 is ruled unconstitutional

When California's so-called Proposition 22 passed in November 2020, many felt that drivers and couriers had been taken for a ride by the companies that lobbied for the new rules. But now, the tide has turned again.

Proposition 22 is a ballot measure which allowed companies to continue treating Californian gig workers as independent contractors, giving them minimal rights relative to what employees have a right to. The measure overrode a 2019 state law and a 2018 State Supreme Court ruling, which would have forced companies to reclassify their workers as employees.

What followed in the space of almost a year was a legal battle that has finally awarded workers a win: The Alameda County Superior Court ruled that Proposition 22 is unconstitutional.

'A prohibition on legislation authorising collective bargaining by app-based drivers does not promote the right to work as an independent contractor, nor does it protect work flexibility, nor does it provide minimum workplace safety and pay standards for those workers,' the judge wrote. Proposition 22 is now unenforceable.

Companies react

In a statement, the coalition representing the gig economy companies, called the Protect App-Based Drivers and Services, said the companies planned to appeal. No surprise, given how much they invested in lobbying in the lead-up to the Proposition 22 ballot vote.

In parallel, there's another ballot measure brewing in the USA. In August, the Massachusetts Coalition for Independent Work filed a ballot proposal to create a new class of workers in Massachusetts. The coalition, which includes Uber, Lyft, DoorDash, and Instacart, aims to make voters decide in 2022 whether gig workers should be considered independent contractors. The coalition proposes that gig workers be exempt from being classified as employees, but entitled to some limited advantages, such as minimum pay.

Staying true to form

Last February, we wrote on how indispensable gig economy workers have become since the pandemic's outbreak. We quoted from Uber's own white paper, *A Better Deal*, which explained how 'drivers were there to help safely transport tens of thousands of health workers', and how 'couriers provided an essential delivery service and a lifeline for local restaurants'. Now that the culture of shared taxis and home deliveries has set in and is likely to stay, it's even more critical that workers are well-protected.

The private sector claims that most of their workers prefer the flexibility of independent work, rather than being tied down as employees. Workers are told they can't have both. The best way for policymakers to determine what workers want is to ask them or their unions directly, or at least, launch public consultations where workers can voice their opinions.

Until then, it's still too early to determine what the best formula should look like. Around the world, the patchwork of legislative models is as colourful as it gets.

Yet, whether gig workers vie for flexibility or security (or both), their working conditions should match the label. Self-employed workers are typically able to set their own prices while employees are able to rely on paid vacation leave, sick leave, and other social security protections. Gig workers often get none of the above.

Any third classification in the making should not be a tool for companies to impose their terms on workers, while casting aside their responsibilities as employers. The maxim that 'you can't have your cake and eat it too' applies to everyone, not just the workers.

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 the past few weeks. For other event reports, visit the Past Events section on the *GIP Digital Watch* observatory.

GGE Lethal Autonomous Weapons discussions 3–13 August 2021

The first session of the 2021 Group of Governmental Experts (GGE) on emerging technologies in the area of lethal autonomous weapons systems (LAWS) considered the recommendations that parties submitted earlier in the year with regard to the existing normative framework. The second session is expected to take place from 27 September to 1 October.

The 2021 Innovations Dialogue: Deepfakes, Trust And International Security 25 August 2021

The session discussed how algorithmically-generated synthetic visual and textual media is created and disseminated, and how such materials could erode trust and present novel risks for international security and stability. Governance issues regarding deepfakes and their technological countermeasures were also considered. The participants debated whether new multilateral and multistakeholder tools are needed to fill the governance gaps.

The Artificial Intelligence and Internet of Things Tour 30 August 2021

The roundtable discussion, organised by the Geneva Internet Platform as part of the series 12 Tours to Navigate Digital Geneva, explained how Geneva gathers multiple actors working on AI, creating a unique ecosystem for interdisciplinary and cross-sectoral digital governance. Diplomats and international officials should take advantage of the many opportunities that Geneva offers when it comes to building capacities on AI and digital governance. Moreover, despite the current efforts by many international organisations, there is a pressing need to connect the dots among both national and international expertise incubators, and to foster cooperation on AI applications and more widely on digital technologies.

What to watch for: Global digital policy events in September

Let's look ahead at the global digital policy calendar. Here's what will take place next month around the globe. For even more events, visit the Events section on the *Digital Watch* observatory.

13 Sep–1 Oct, Human Rights Council 48th session (Geneva, Switzerland)

The Human Rights Council will consider the annual report of the United Nations High Commissioner for Human Rights, and reports of the Office of the High Commissioner and the Secretary-General. It will also discuss the promotion and protection of human rights, human rights situations in several countries, and combating racism, racial discrimination, xenophobia, and related forms of intolerance, among other topics.

September

14–15 Sep, 2nd AI Policy conference (online)

Organised by RegHorizon and ETH Zurich's Center for Law and Economics, the conference will tackle three key themes: (a) Implications and gaps of current regulatory proposals and soft law approaches for AI technologies, (b) the possibility of new technologies and innovative approaches to accelerate business readiness and ensure higher effectiveness of AI policy, and (c) building awareness and inclusive engagement of the developing South, youth, and civil society.

14–30 Sep, UN General Assembly 76th session (New York, USA)

The 76th session of the UNGA will open on 14 September with a high-level meeting themed 'Building resilience through hope – to recover from COVID-19, rebuild sustainability, respond to the needs of the planet, respect the rights of people, and revitalise the United Nations'. The general debate on this topic will run from 21 to 30 September 2021.

As usual, we'll analyse the digital policy priorities identified by the Heads of States in their speeches during the General Debate. Our analysis will be available on the Digital Watch observatory.

28 Sep–1 Oct, WTO Public Forum 2021 (online and Geneva, Switzerland)

The 2021 edition of the WTO Public Forum is themed 'Trade Beyond COVID-19: Building Resilience', and will look at how the multilateral trading system can help build resilience to COVID-19 and future crises. The forum will have three subthemes: Enhancing resilience beyond COVID-19, strengthening the multilateral trading system, and collective action towards sustainable trade.

October

About this issue

Issue 62 of the Digital Watch newsletter, published on 15 September 2021 by the Geneva Internet Platform and DiploFoundation | Contributors: Stephanie Borg Psaila (editor), Ana Maria Correa, Andrijana Gavrilović, Marco Lotti, Virginia (Ginger) Paque, and Sorina Teleanu | Editing and design: Aleksandar Nedeljkov, Viktor Mijatović, and Mina Mudrić | Get in touch: digitalwatch@diplomacy.edu

On the cover

Taliban's e-rise. 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