Carina Perkins, and Yoram Wurmser

The Daily: How the EU's AI Act is—and isn't—informing US legislation, the era of BadGPTs, and a BNPL credit card

Audio

On today's podcast episode, we discuss the most important parts of the EU's new AI Act, what's missing, and how these rules could shape US regulation. "In Other News," we talk about what nefarious GPTs can get up to and a card-linked buy now, pay later (BNPL) offering. Tune in to the discussion with our analysts Carina Perkins and Yory Wurmser.

Subscribe to the "Behind the Numbers" podcast on Apple Podcasts, Spotify, Pandora, Stitcher, YouTube, Podbean or wherever you listen to podcasts. Follow us on Instagram

Episode Transcript:

Marcus Johnson:

This episode is made possible by Nielsen. Sharpen your media planning with Nielsen's Upfronts NewFronts Guide. Whether it's linear TV or streaming. Nielsen helps you optimize,

reach and impact. Visit nielsen.com for more information.

Carina Perkins:

Similarly, chatbots are considered limited risk, and on the whole they probably are, but just labeling that something is not human isn't necessarily going to negate the potential risk involved with that chatbot.

Marcus Johnson:

Hey gang, it's Tuesday, March 12th. Carina, Yory, and listeners, welcome to Behind The Numbers Daily, an eMarketer podcast made possible by Nielsen. I'm Marcus, today I'm joined by two people. The first of those two is principal analysts who covers everything advertising, media and technology based in New Jersey. It's Yory Wurmser.

Yory Wurmser:

Hey Marcus, how are you doing?

Marcus Johnson:

Hey fella, very well, how are we today?

Yory Wurmser:

I'm doing great.

Marcus Johnson:

Very good. We're also joined by one of our senior analysts based on the south coast of England, who covers retail and E-commerce with a particular focus on the UK and Western Europe. It's Carina Perkins.

Carina Perkins:

Hi Marcus, thanks for having me back.

Marcus Johnson:

Of course. Today's topic is about EU AI rules and how they will shape US regulation, but we of course start with today's facts. And Carina, this one's for you. It's the UK facts and facts about Buckingham Palace. So, according to the Royal website, Buckingham Palace has

served as the official London residence of the UK Sovereign since 1837. And today it is the administrative headquarters of the Monarch, although in use for the many official events and receptions held by the king, the State Rooms at Buckingham Palace are open to visitors every summer. Buckingham Palace has nearly 800 rooms, including 188 staff bedrooms, 92... Imagine how cool it would be to say you worked and slept there, it'd be cool, wouldn't it? Probably for a week and then like, uh.

Carina Perkins:

Yeah.

Marcus Johnson:

92 offices, 78 bathrooms, 52 Royal and guest bedrooms, 19 State rooms. The palace measures 830,000 square feet. So it'd be 140 times larger than the average American home. It's got everything.

Carina Perkins:

Do you know how many times larger it would be than the average UK home?

Marcus Johnson:

Probably a billion. I couldn't find a good average, but our houses are small.

Carina Perkins:

Much smaller.

Marcus Johnson:

Yeah. The palace is everything it needs to be its own self-sufficient village. It's got a post office, movie theater, police station, clinic.

Carina Perkins:

A police station?

Marcus Johnson:

Yeah, why has it got a... I guess probably just a place where the police hang out, no one's going down and reporting, oh, the Prince was yelling at me again.

Carina Perkins:

Yeah.

Marcus Johnson:

We'll go and talk about [inaudible 00:02:52].

Carina Perkins:

Surely they've got their own police, or they are the police.

Marcus Johnson:

Yeah, exactly. Yeah, because she's on everything. Well, he'll be on everything eventually.

Carina Perkins:

Well, she was, yeah.

Marcus Johnson:

Well, the Queen's face is on everything. Charles's face will soon be on everything, but if you're on the money, you can do what you want. Over 50,000 people visit the palace each year as guests to State banquets, lunches, dinners, receptions, and garden parties. I'm yet to be invited.

Carina Perkins:

My mom's been to a garden party.

Marcus Johnson:

What?

Carina Perkins:

Yeah.

Marcus Johnson:

Really?

Carina Perkins:

Yeah.

Marcus Johnson:

Without me? How'd she get invited and how can I?

Carina Perkins:

She used to work for a charity that was supported by Prince Edward.

Marcus Johnson:

I'm not that [inaudible 00:03:32]. All right.

Carina Perkins:

One day Marcus, one day.

Marcus Johnson:

Probably not. Anyway, today's real topic, how the EUs AI Act is and isn't informing US regulation.

In today's episode, first in The Lead, we will cover how AI is being regulated across the pond. I sound English, so you think I'm in the UK, but via across the pond, I mean the UK because I'm in America. Then for another news, we'll discuss the era of BadGPTs and Amex introducing a card linked Buy Now, Pay Later offering. We start, of course, with The Lead, and we're talking about what's going on across the ponds in Europe when it comes to AI legislation. Towards the end of last year, the EU block of 27 countries reached a landmark deal on the world's first comprehensive AI regulation. And notes Kia Kokalitcheva of Axios. The AI Act, as it's called categorizes AI uses according to four risk levels with increasingly stringent restrictions, the greater the potential risks. What's in the law? Well, Ryan Heath of Axios did a fantastic job of outlining some of the main parts, so I didn't have to read it.

So, what do we have here? We've got the EU law bans several uses of AI, think bulk scraping of facial images and most emotion recognition systems in workplace and educational settings. Number two, it bans controversial social scoring. These are evaluations of compliance or trustworthiness of citizens. Number three, it restricts facial recognition technology in law enforcement to a handful of uses like IDing, victims of terrorism, human trafficking and kidnapping. AI companies will need to submit details of the training data they

used to build these models. Operators of systems creating manipulated media will have to disclose that to users. And another point here, providers of high risk, what they call high risk AI, especially in essential public services, will be subject to reporting and have to make data available to the public and human rights impact assessments as well. Penalties for this, companies violating the rules could face fines of $38 million.

That's 35 million euros. I don't know if it's per violation or total, I'm not sure how that works or a fine of between 1.5% to 7% of global sales. EU national governments are exempt from some aspects of the law for military or defense uses of AI. And finally, the EU is still ironing out some of the details and they also still have to vote on the law. It's a formality at this point, it seems like everyone's going to say yes. The rules won't take effect though until 2025 at the earliest. But Carina, I'll start with you, which part of this legislation do you think or parts do you think are most important?

Carina Perkins:

I think it's probably the part where it just completely bans AI systems that pose an unacceptable risk. So, those are systems that it deems to contravene EU values and poses a threat to people's fundamental rights. So, as you mentioned that things like untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases or social scoring or AI systems that are manipulating human behavior to circumvent their free will. So, I think actually that kind of total ban on those sorts of systems is probably the most important part of it.

Marcus Johnson:

Yory, what about for you?

Yory Wurmser:

Yeah, I think that total ban's important. I think the tiering of the risk level and also by size. So, the general AI models that are going to be most regulated are the extremely large ones, and it really probably is limited to OpenAI's GPT-4 and Google's Gemini giant models like that. And open source models seem to have a much lighter requirement level so, that's an interesting distinction as well.

Marcus Johnson:

What's missing? What's the greatest omission from this EU AI Act?

Carina Perkins:

I think the thing that concerned me the most was the very light touch that they're applying to deep fakes. So, they would come under the limited risk category, and that's just some regulation around transparency so it requires creators to be transparent. Anyone who creates or disseminates deepfake has to disclose that it's artificial and provide some information on what technique was used to produce it. And I don't think that labeling it is always going to be enough to combat the potential harm that they can cause, and there's also still some uncertainty around the legal liability and exactly who would be responsible in the case of misuse.

Marcus Johnson:

Right.

Carina Perkins:

Similarly...

Marcus Johnson:

And also, you can get rid of watermarks, right?

Carina Perkins:

Exactly.

Marcus Johnson:

I believe it's pretty easy to remove them, it sounds like.

Carina Perkins:

And if someone's using deepfakes for malicious purposes, they're the most likely to then ignore the law, aren't they?

Marcus Johnson:

Right.

Carina Perkins:

So yeah, I think, and similarly, chatbots are considered limited risk, and on the whole they probably are, but just labeling that something is not human isn't necessarily going to negate the potential risk involved with that chatbot. So I think there was a case in Belgium where a man committed suicide after conversing with a chatbot who encouraged him to sacrifice himself to save the planet. So, there are risks out there that even if people know they're not conversing with a human, that doesn't necessarily negate all of the risks. I think that kind of minimum safety safeguard for AI systems isn't quite addressed by the legislation as it stands.

Marcus Johnson:

Wasn't there a case... Wasn't that the chap in the UK who, speaking of Buckingham Palace, I think he broke into Buckingham Palace and he had a crossbow and he was trying to get to, at the time the Queen, this is 2021 and they said, why were you doing this? And I believe that was the case where he said he'd been talking to a chatbot and the chatbot had helped to convince him that he could do anything he wanted, pretty much. He'd been asking questions and it had been saying, yeah, you are the best. You're able to do whatever you want. And yet, he wasn't able to distinguish between... And it led to some pretty grave consequences.

Carina Perkins:

And as far as I understand, the AI Act doesn't put kind of guardrails around that. It assumes that if people know that they're not conversing with a human, that will mitigate the harm, I don't think it does.

Marcus Johnson:

Yeah. Yory, what's missing from this for you?

Yory Wurmser:

Well, I mean some of it is just part of the process and the specific regulations, specific requirements, those are going to be stipulated by the AI office that it has to be formed. The EU has to hire people for that office, has to set it up, and then they have to set the rules. And with GDPR a few years ago, it was those rules, where the details and those rules where everything turned on. Until those rules are laid out and detailed, there's not going to be a lack of clarity exactly what's expected of companies, and I think that, at this point is still missing.

Marcus Johnson:

One of my biggest concerns here was how quickly these rules can become out of date, because the rules won't take effect until 2025 at the earliest. Jess Weatherbed of the Verge thinks it might be mid 2026 by the time we see everything within the AI Act regulated. So, that's at least nine months if you're talking start of 2025 from today. Maybe over two years from nine months to two years, these things could actually completely go into effect. How quickly will things change from now until then? How different will the landscape be knowing ChatGPT came out just over a year ago and the EU has been working on this version of the AI rules for the last three years. So, are you surprised that nothing's going to happen until at least nine months in the future?

Carina Perkins:

I'm not surprised because this is just the pace at which regulation happens. I think that's the biggest challenge with regulating something like AI where the technology is developing so quickly. Regulations can't really keep pace with it. And it's where in some instances I think we're going to be relying on existing regulations, so things like GDPR, but that's obviously not going to cover all of the issues that might arise from the technology.

Marcus Johnson:

I just wonder how much of this is going to be invalid. What share of this by then. Let's turn our attention to the US because a lot of the time Europe will set the standard for regulation on certain things and then the US, often California first, will peak over the pond, say, what are you up to? Oh, interesting. That looks good. And adopts some of those practices in the US in a singular State, and then that spreads throughout the country. We've seen that with a lot of different types of rules, GDPR, privacy rules, things like that. And so, turning our attention to America, Kim Mackrael of The Journal writes, countries around the world actually have struggled with weather and how to regulate AI. She first reminds us that Chinese regulators earlier this year issued rules dealing with GenAI. In the US, the Biden administration in October issued an executive order on AI safety that we covered at the time.

At the start of the year, the White House said the AI regulation process is well underway, releasing an update to AI regulations following President Biden's 2023 executive order. I believe that was a 100-page document. Ben Sherry of Inc. explains the updated rules include the following. One, the Defense Production Act will force developers of powerful AI systems to send the government information about the results before the new version gets released to the general public. Number two, the government will hire more AI experts across federal

agencies. Number three, a set of responsible AI use guidelines, like designating a Chief AI Officer establishing internal mechanisms for working on large scale AI projects with multiple stakeholders and conducting AI impact assessments before and after experimenting with the technology. So, a set of guidelines being issued. But Yory, I'll start with you. What do you make of where the US currently stands with its efforts to regulate AI?

Yory Wurmser:

Well, it's way behind Europe. The guidelines set forth by the Biden administration are mostly about US agencies. You really need Congress to pass a law for a full regulation or States, but something as complicated as this, it's really probably going to come down to a federal law. But in the meantime, a little bit like existing regulations in Europe cover some of the facets of AI regulation already, I think in the US, some privacy laws, the FTC and courts will probably have some hand in what companies can do through just rulings on copyright infringement or use of private data or personal data. So, I think even before you get federal regulations, you're going to get some court rulings and some FTC rulings on this, but where we're behind is just the federal regulation.

Marcus Johnson:

You mentioned copyright. Stay tuned for an episode coming out March 19th where myself, Yory and Evelyn Mitchell-Wolf will be talking about AI and copyright and where the copyright laws could actually torpedo a lot of the GenAI hype at the moment. Carina, what do you make of where the US stands in comparison to the EU?

Carina Perkins:

Yeah, I agree with Yory that the US is way behind. It's taking a more cautious approach. I think it's concerned that stringent rules could make US companies non-competitive. I think it's really interesting how far behind it is given the difference in investment in AI. So, I saw a deal room study that shows that in the US between 2019 and 2023, there was 23.8 billion in generative AI VC investment. And in Europe it is 1.8 billion.

Marcus Johnson:

Wow.

Carina Perkins:

Yeah. So I thought that was an interesting point.

Marcus Johnson:

Yeah, that is a lot more.

Carina Perkins:

Interestingly as well, the UK also is taking a similarly more light handed approach. It's very concerned about stifling innovation and introducing a whole new regulatory regime. So, it's also not going to be as stringent as the EU. The EU is not afraid of imposing stringent legislation. So it doesn't surprise me that it's leading on this.

Marcus Johnson:

Yeah. Well, we talked about the EU, it's easy to forget that the UK is no longer part of the EU, and so, where does the UK stand? Where do you think they're going to fall in terms of getting something passed and how strict that legislation will be?

Carina Perkins:

They're not at the moment, there was a white paper on a pro innovation approach to AI regulation, which was presented to Parliament in, I think March 2023. That doesn't propose the creation of new laws or any empowerment of a new regulator, but it's empowering existing regulators with responsibility for establishing sector-based approaches to the way that AI is impacting on their individual sectors. So, it's taking a very different approach to the EU.

Marcus Johnson:

I thought they'd be further along, I'm quite surprised by that. But I guess they probably thought that they were going to just use the EU's version.

Carina Perkins:

No, I don't think they did. I just think the government is afraid of taking a anti-technology approach. It's very pro technology, it's very pro innovation. I don't think it wants to stifle that.

Marcus Johnson:

Okay.

Carina Perkins:

But yeah, it's definitely taking at the moment, a lighter touch to AI than the EU.

Marcus Johnson:

Okay. So I guess, yeah, we left the EU in January 2020, so I thought that maybe we're just thinking, oh, we'll use the EU version of rules, but didn't start working on those until the year after. All right folks, that's all we've got time for, for The Lead time now for the second half of the show. Today, in other news. Welcome to the era of BadGPTs and American Express brings a card linked, Buy Now, Pay Later offering to the UK.

Story one. Welcome to the era of BadGPTs writes Belle Lin of the Journal. She notes that a new crop of evil chat GPT cousins, called things like FraudGPT are being made to turbocharge phishing emails and create better deepfakes. In one example, Ms. Lin points out that earlier this year, a Hong Kong multinational company employee handed over $25 million to an attacker who posed as the company's chief financial officer on an AI generated deepfake conference call. The South China Morning Post reported citing Hong Kong police. Yory, what is your greatest concern when it comes to these BadGPTs?

Yory Wurmser:

Yeah, we've all been through training where we look for phishing attacks, misspellings, and so forth. I mean, the first obvious thing is just that the language is going to be better. So it's going to be much harder to identify not just the language, but the techniques will be much more aware of malware identifying software can evade them, but more nefariously, spear phishing attacks. So attacks that are meant to impersonate someone or directed towards an individual with individual information, those are going to become a lot easier to do. And that's what happened in Hong Kong where someone was impersonating... A bot was impersonating another executive, and that just becomes super hard to identify and prevent so, it's really dangerous.

Marcus Johnson:

Yeah. The thing that leapt out to me was that GenAI really turns on the fire hose because the article is pointing out phishing emails grew by over 1,000%. It's not like there were no phishing emails before generative AI came about. There are plenty, there are enough. And now it's grown by over a 1,000% in the 12-month period starting when ChatGPT was publicly released

with an average of 31,000 phishing attacks sent every day, according to an October 2023 report by cybersecurity vendor SlashNext.

Story two. American Express brings card linked Buy Now, Pay Later offering to the UK to capture the growing demand for installment payments. Our Senior Payments Analyst, Grace Broadbent, how does the Plan It, as it's called, Plan It card work? Grace explains that card holders can select a transaction or an amount from their recent statement to pay in installments across three, six or 12 months. Users are charged a fixed monthly fee, but pay no interest on the balance of the installment plan. She notes. But Carina, what do you make of this new offering from Amex that apparently got launched in the US six, seven years ago, but is now in the UK?

Carina Perkins:

So, I don't think it's surprising that they've launched this at all. We've seen massive growth in Buy Now, Pay Later adoption in the UK. Part of that's been driven by the cost of living crisis, but I think also players such as Klarna are really pushing it in the UK. Buy Now, Pay Later volumes expected to account for 12.1% of UK E-commerce payments by 2025. So, it's really fast-growing and a lot of people, especially younger generations, are using Buy Now, Pay Later instead of credit cards because it's interest free for that kind of installment period. And I think that the credit card companies are now really having to catch up with that and offer something similar.

Marcus Johnson:

It seems like Buy Now, Pay Later is nearly as popular in the UK as the US. We don't have UK numbers, but our forecasting team think 29% of Americans over 14 used Buy Now, Pay Later last year. So 29%, only slightly more than the 27% of UK adults who used Buy Now, Pay Later at least once in the six months prior to January. That's according to the UK's Financial Conduct Authority.

That's all we've got time for, for this episode. Thank you so much to my guests. Thank you to Carina.

Carina Perkins:

Thanks Marcus.

Marcus Johnson:

Thank you to Yory.

Yory Wurmser:

Glad to be here.

Marcus Johnson:

And thank you to Victoria who edits the show. James, who copy edits it. Stewart runs the team, Sophie does our social media, and thanks to everyone for listening in to the Behind The Numbers Daily an eMarketer podcast made possible by Nielsen. You can tune in tomorrow to the Reimagining Retail Show with host Sarah Lebow as she speaks to our Zak Stambor and Becky Schilling all about Walmart.