GENERATIVE AI HUB

AI agents are coming to Europe. The rules to let them in are not

London and Brussels have told the makers of AI agents to play by the rules. Neither have said on what terms websites and devices should let them in.

Dr Christophe Carugati · 19 November 2026

On 16 November, Britain's four digital regulators, who work together as the Digital Regulation Cooperation Forum (DRCF), told ministers that several personal AI agents are about to launch in Britain. Their message to the firms behind them: engage early and meet your obligations before launch. The regulators are right to worry. Elsewhere, the agents are already here.

Within six weeks of its launch, more than 10 million people in the US and Canada set up Meta Muse, an artificial intelligence (AI) agent that shops, books and pays on their behalf, says Mark Zuckerberg, Meta's chief executive. Muse has yet to reach Britain or the EU. When agents like it arrive, they will find a web built for humans, and no clear rules on when to let them in. The UK regulators' letter outlines the obligations AI agent makers must meet, but not the terms websites and devices should set to admit them. Nor does the Digital Fairness Act, proposed on 11 November, which allows a shopper to set limits on their agents, say how a website should treat them.

Agents are not people. Where humans look at a website, agents simply read it: no eye drawn to a banner ad, no impulse to add one more item to the basket. They make mistakes no person would, such as ordering the wrong item. Worse, they can hand a home address to a stranger, or act on a bank account without instructions. In short, a helpful assistant can quickly become an economic, privacy and security problem.

Some websites are fighting back. United Airlines bars agents from booking entirely, citing privacy, security, and aviation rules. Cloudflare, an internet infrastructure firm that serves a large share of Europe's online businesses, began blocking AI agents by default in September on pages that display ads, leaving website owners to negotiate terms of access.

Concerns about privacy and security are legitimate. But there is a commercial motive too, which Cloudflare admits openly: ads are made for human eyes, and agents skip them. Blocking keeps control of the consumer experience, and of the revenue streams that come with it.

Websites' actions point to who is controlling the door to agents. The latter are useful only if websites let them in, and websites will do so only if they can trust them. A group of international banks says shopping by agents can work only with common standards, clear liability and strong data protection.

Britain's regulators have made clear that existing law already applies to agents. Brussels has gone further, at least on access to certain devices.

In July, the European Commission ordered Google to give rival agents the same access to Android phones' features and data as its own agent, Gemini. Some of the most sensitive features may be restricted to certified agents. Those conditions bind Gemini, too.

How, then, should websites and devices open the door in a way that builds trust? Two steps, for both sides of the door, would help.

The first step is security. The technology behind agents is immature. France's cybersecurity agency, ANSSI, warned in April that agents on desktop computers pose significant cybersecurity risks, and advised keeping their permissions to the strict minimum. Britain's regulators, for their part, say agents must not disrupt the wider systems they plug into. In practice, websites and devices should let agents browse and compare freely, while keeping them away from websites and features that expose sensitive data, such as bank accounts or a phone's screen, until agent providers can show safeguards that meet legal obligations or defined industry standards. And whoever opens the door must also be able to close it again on an agent that breaks the rules, which is why the regulators are right to expect continuing engagement with firms after launch.

The second is for the firms building agents to work together on safety. Some AI bosses, including Anthropic's Dario Amodei, have proposed shared safety standards among leading AI companies, backed by governments and exempt from competition law. Yet such collaboration could slow progress and harden into a cosy club that shuts out rivals. Competition authorities should therefore help shape the standards, so that safety does not become a barrier to entry. In Britain, the natural forum is the DRCF; in the EU, the European Commission.

These steps are the bare minimum to keep markets open, data private and systems secure. Above all, regulators in London and Brussels should work with industry to spell out the terms on which websites and devices let agents in, and use regulatory sandboxes currently being established to test them. Get this wrong, and agents will be either locked out or let loose. Neither would build the trust agents and the people who use them need.

DISCLOSURE

Christophe Carugati founded Digital Competition, a consultancy and think tank organisation focused on digital and competition policy. His clients include Amazon, Alphabet and Apple; the views expressed here are his own.

About

DIGITAL COMPETITION

Digital Competition (https://www.digital-competition.com/) promotes digital and competition policies that foster innovation. We combine legal, economic and policy expertise to deliver cutting-edge research, training, strategic advice and high-impact regulatory intelligence.

Led by Dr Christophe Carugati, with a decade of deep expertise in digital and AI markets, we address the most pressing challenges in the rapidly evolving digital and competition policy landscape, impartially, rigorously and with a commitment to actionable recommendations.

The views, analyses and recommendations are solely those of the author, not those of his clients.

This analysis is part of our Generative AI Hub (https://www.digital-competition.com/generativeai). We assess competition issues raised by Generative AI, from foundation models to answer engines and agentic commerce.

Contact us for service, membership, training or press enquiries.



DR CHRISTOPHE CARUGATI

Dr Christophe Carugati (christophe.carugati@digital-competition.com) is the founder of Digital Competition. A leading expert on digital and competition policy, he is known for impartial, high-quality research. He holds a PhD in law and economics, with a thesis on big data and competition law. He was previously an affiliate fellow at Bruegel, an economic think tank, and a lecturer in competition law and economics at Lille University.