Tap with care

Dr Christophe Carugati

Britain's competition regulator wants to open the iPhone's contactless chip further. It should clarify fee principles, curb over-prompting and let Apple set and enforce security standards for new uses.

Britons tap for almost everything, from paying for train tickets to unlocking their cars. Ever more of those taps come from phones. In 2025, 58% of British adults regularly paid by mobile, according to the Competition and Markets Authority (CMA), the UK's competition regulator. Now the CMA plans to use its digital competition regime to change how Near Field Communication (NFC), the technology behind each tap, works on Apple's iPhones. The CMA hopes this will let developers improve their apps and build new contactless services, from payments to digital car keys. The trick is to do so without blunting firms' incentives, Apple's included, to provide the technology, or compromising users' security.

Start with the technology. Phones can use NFC to mimic a card in two main ways. Host Card Emulation (HCE) runs in software and relies on credentials stored remotely, so it must reconnect to the internet regularly. Secure Element (SE) keeps data on a dedicated chip inside the handset, so it works even offline. Apple argues that SE is more secure, and the CMA acknowledges that it may be better suited to some uses, such as digital car keys. That is why Apple gives developers access only to SE through a platform it has offered in Britain since October 2024. The CMA wants to go further by adding HCE as a second route and regulating the terms of both.

Apple has opened up HCE before. In the European Union, under commitments agreed with Brussels in 2024, it already does so free of charge. Rival payment apps from Vipps, PayPal, Klarna, Curve and BBVA soon followed. The CMA wants HCE opened in Britain too, because HCE makes contactless apps faster and cheaper to build. Unlike Brussels, though, it would let Apple charge fair fees for both HCE and SE. Apple objects that this would override its technological choices and blunt its incentive to invest in SE. The CMA retorts that access to both would let developers offer a wider choice of secure services. Apple also asks why it should support a second technology that its own wallet does not use. But the real fight is less over which technology developers use than over what they pay for it and on what terms.

The CMA reckons Apple's fees for SE access are too high for many contactless services to be commercially viable. It wants to rewrite both price and terms.

Take price first. The CMA's plan sets no fixed fee. Rightly so. It wants flexibility for very different uses and business models, and to preserve Apple's incentive to innovate. Instead, it sets out principles for fair and reasonable fees, which it expects to be lower than today's. Applying them will be hard, as the CMA admits. Apple would have to weigh factors such as its market power and the value it and developers bring to each other. The CMA would do well to clarify how the principles apply, with clear metrics, so that Apple can set its fees with confidence that they comply.

Then come the conditions, starting with default apps. Being the default brings perks, such as opening automatically when an iPhone is held near a contactless reader. Developers can already prompt users to switch. The CMA wants Apple to go further and let them check whether their app is the default, with no limit on how often they can do so.

Brussels took a different line. The European Commission did not require Apple to give developers access to a register of default apps, judging that it might be out of scope, hard to implement and of little added value. It may have a point. If the goal is simply to let users pick a default app, letting apps prompt them to flip a simple switch in the iPhone's settings may be enough. Yet without such a signal, developers counter, they cannot tell whether their app is already the default, and so risk pestering users. The risk is real. Too many prompts breed fatigue, as anyone who has clicked through endless cookie banners knows. The CMA sides with developers, arguing that they have little reason to nag users and that Apple's App Review Guidelines on user experience already act as a safeguard. Even so, the regulator would be wise to cap how often apps can check, much as Apple already does for browsers, to guard against over-prompting.

Last comes the question of who gets access, and who keeps it. The CMA proposes that Apple grant access to all developers, though it may refuse or withdraw it from those that breach applicable laws or industry standards. Once access is granted, Apple may suspend it only temporarily, where such a breach causes or credibly threatens serious harm, and must be able to justify doing so to the CMA. But it can act without notice, which should let it respond swiftly. Where new uses lack an established standard, Apple must still grant access, but can require developers to show, with objective evidence, that their approach offers privacy and security protections proportionate to the risks. That leaves Apple little room to refuse, even if it thinks another approach would protect users more effectively.

Better for the CMA to let Apple, which knows best how to keep the iPhone secure, propose its own alternative standards in such cases, and to suspend access where developers breach those standards or depart from the approach they set out to win access.

The CMA has struck a sensible balance in its bid to spur competition. Though it mandates a second technology, it allows reasonable access fees, sets fair conditions and lets Apple suspend access when needed. But its plan asks a lot of Apple, which must redesign its NFC set-up for Britain. Clearer fee principles, a curb on over-prompting and a say for Apple over security standards for new uses would lighten that load. Without them, opening up the iPhone's tap could fall flat.

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, which include Apple.

This analysis is part of our Digital Competition Regime Hub (https://www.digital-competition.com/digitalcompetitionregime). We provide research on the design, implementation and enforcement of digital competition regimes worldwide, from the EU DMA to the UK DMCC Act.

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.