22 April 2026

Comments of

TRUSTED FUTURE

To the

United Kingdom's Competition and Markets Authority (CMA)

regarding its

Open call for evidence regarding

Recent developments in relation to Apple's and Google's app store rules

On behalf of **Trusted Future,** a non-profit organization dedicated to the belief that we need smart well-informed policies to enhance trust throughout today's digital ecosystem, we welcome this opportunity to provide input to the Competition & Markets Authority (CMA) on its call for evidence on recent developments relating to Apple's and Google's app store rules.

The CMA has an opportunity to build upon the trust that has proven to be essential to enabling the UK's thriving, innovative, and essential mobile ecosystem. To do so we encourage the CMA to use an evidence-based approach to identify demonstrable competition failures, specific consumer harm, proven interventions and to fully evaluate the necessity, efficacy and risks associated with any proposed intervention. To continue to drive trust deeper into the mobile ecosystem, it should ensure that any proposed interventions never weaken, but continue to advance the privacy, safety, and security safeguards necessary for UK progress.

At a time of such dynamic change, when trust in digital ecosystems is being challenged nearly every day, and trust has emerged as a central enabler for digital adoption, a non-pretextual procompetition differentiator, and a basis for consumer gains, we believe it's vital that any measure that CMA considers in this domain be reviewed through a lens of trust. This will help ensure that UK users are able to take full advantage of a vibrant mobile digital ecosystem that is innovative, safe and secure, competitive and trustworthy — an ecosystem where people are able to improve their lives because they have access to trustworthy technologies that protect their privacy, safety and security.

There is much to learn from recent international developments. Recent international regulatory developments — particularly those in Europe, Japan and the US — highlight the important steps that companies must take to instill trust in their technologies, and how certain regulatory interventions have the potential to undermine/disrupt the vital trust that is necessary for UK users and businesses to benefit from mobile opportunity. As explained in more detail below; to avoid regulatory missteps, the CMA should consider several core issues:

1. The CMA should look at these issues through the lens of trust. In 2022, the UK's DCMS review into app security and privacy outlined key objectives for the UK, including that, "[a]ny future regulation that changes the app ecosystem should understand the impact on cyber security." It was also concerned about risks to privacy, and suggested that the "The UK government is therefore keen to ensure that changes to the app store ecosystem do not create significant new security risks to users." Although several years have passed since this assessment, the importance of infusing greater privacy, safety and security into the mobile app ecosystem has only become more important. We see that the CMA has acknowledged "the potential for lower security and privacy protections" in its solicitation and believe CMA should continue to advance, and not weaken, the robust privacy, safety and security that are essential for a trusted mobile digital ecosystem.

2. To do so, CMA should take the time necessary to identify and address actual consumer harms, with evidence-based solutions that specifically address the identified harms to produce corresponding consumer benefits. In doing so, it should consider the necessity, efficacy, and risks associated with any steering remedy. And in the process of considering interventions, fully explore the possible hazards, and unintended consequences of those actions — and whether there are appropriate mitigations that can overcome such risks in order to maintain trust.

3. To help support CMA's call for evidence, we explore in more detail below how:

    A. Trust has become an essential infrastructure upon which UK digital opportunity is built.

    B. A trustworthy mobile ecosystem provides enormous benefits to UK's developers.

    C. Existing integrated billing systems are an important enabler for trust in the UK.

    D. UK developers have concerns about alternative billing systems, and their direct impact on consumers and adoption.

    E. There is no demonstrated consumer harm that warrants additional steering intervention.

    F. Europe's DMA link-out strategy highlights critical privacy, safety and security risks for users.

    G. Link-out provisions can undermine efforts to block scams and fraud.

    H. Link-outs can undermine a parent's ability to protect their children.

    I. Link-outs don't foster new competition.

    J. Interventions to lower commission fees do not lower app prices or create consumer savings.

    K. Static text is a safer alternative to active link-outs.

    L. How Japan addressed some of the most significant privacy, security and child safety weaknesses inherent in Europe's approach.

Regulations that lack sufficient market evidence to prove their efficacy, undermine the cognizable procompetitive security ecosystem restrictions, or that don't address specific consumer harm with proven remedies, are more likely to harm the groups they aim to serve. In

this case, **Trusted Future believes that the preponderance of evidence, as well as the unintended consequences seen from actions in the EU and US, demonstrates a lack of efficacy, and therefore believes that no intervention is warranted or necessary in the UK at this time.**

A. Trust has become an essential infrastructure upon which UK digital opportunity is built.

In October 2023, the UK Government published an updated version of the voluntary Code of Practice setting out the baseline security and privacy requirements for app store operators and app developers — helping to advance and ensure baseline levels of trust in the app store ecosystem. As a result of these and other efforts by smartphone manufacturers to build privacy, safety and security into their technologies by design, the mobile ecosystem has become a cornerstone of the British digital economy. UK mobile data consumption has surged, up 495% between 2018 and 2025, driven by more powerful devices, advances in connectivity, and a trusted app economy. In fact, the UK mobile app market has exploded into a £28.3 billion economic powerhouse in 2025, growing at 12.9% annually, and benefitting the 95% of the population that now owns smartphones. This level of adoption and integration into the UK economy has only been possible because of the trust that users and businesses place in their mobile phones.

As mobile devices have become a trustworthy companion, they have become almost ubiquitous throughout our lives. They are now the number one way UK citizens access the Internet. Because they now enable us to do almost anything and everything, UK consumers and businesses now rely on the integrity of their mobile devices and the app ecosystem to protect some of their most sensitive and mission critical aspects of their lives and businesses. They rely on built in privacy and security safeguards so they can trust transactions when they bank, buy, communicate, learn, date, play, and travel. And they rely on these safeguards to protect the extremely sensitive and private information they contain like health data, banking credentials, private photos and communications.

It's not just consumers who rely on their integrity; smartphones have also now become a vital part of the way every sector of the UK's economy operates. They have become so trusted and vital that nearly every UK CEO, critical infrastructure provider, government official, judge and journalist keeps them within reach — in their pockets and purses — at almost all times.

The changes in the way people use this technology have been enabled by massive investments in innovation to build trust into the core of our mobile technologies and a vibrant app ecosystem built upon an app governance system meant to enable trust across the app ecosystem. Increasingly, this trusted mobile ecosystem has proven vital for almost every sector of the UK's economy. Mobile commerce now accounts for roughly 73% of all retail transactions in the UK,

and it is the primary interface for the UK's modern service economy. This major shift in adoption and capability has forced traditional industries (like banking, energy, and retail) to invest heavily in a mobile-first infrastructure which is rooted in trust. Trustworthy technologies, including the integrated payment and transaction systems built into the app ecosystem — have proven to be the foundation upon which global e-commerce, app marketplaces, and UK's digital enterprises are all built.

According to the UK Department for Science, Innovation and Technology (DSIT) Consumer Survey on App Stores, respondents generally have a high-level trust in and usage of app stores. But the DSIT survey also found that the most common impact from an app's security incident was a loss of trust in the affected app (41%), followed by time lost resolving the issue (30%) and emotional or psychological distress (19%). And, a loss of trust in one app undermines the trust of them all. Of those that had experienced a security incident, 65% of respondents agreed or strongly agreed that they were less trusting of apps and took additional actions when downloading apps — and 1 in 5 (19%) respondents stopped downloading apps altogether. DTIS, in an open question, found that after a smartphone user had a security issue, users responded they were "preferring to use well-known or trusted platforms (respondents referred to examples such as the Apple App Store)" and were now minimizing the amount of data shared with developers among other things. (Page 60)

B. A trustworthy mobile ecosystem provides enormous benefits to UK's developers.

A recent survey of UK app developers by MTM found that developers are highly satisfied with both Google and Apple's app stores (providing both with an 8.3 out of 10 satisfaction score) citing value in user growth, security, and monetization. Developers also felt their investment in these platforms was well-rewarded:

- 95% see app stores as important for safeguarding apps from viruses and malware
- 88% believe these app stores cultivate a secure and trustworthy environment for the whole ecosystem, and
- 90% say an app store's approach to user safety and security (e.g. protecting user data, removal of malware) is important to them.

C. Existing Integrated billing systems are an important enabler for trust in the UK.

In the same MTM survey of UK app developers, app stores based integrated billing services received especially high satisfaction scores from developers.

- 84% of developers think it's important that app stores help them monetize their business
- 80% of developers think it's important that app stores provide integrated billing services that deliver a seamless and safe user experience.
- Nine out of 10 developers report that these integrated billing systems are a trusted solution for consumers and businesses for handling end-to-end payment workflows.

- They also report that these payment systems help their companies mitigate fraud and abuse, more easily manage their tax obligations, and manage users.

D. UK Developers have concerns about alternative billing systems, and their direct impact on consumers and adoption.

In the same MTM survey:

- 7 out of 10 developers reported that alternative billing services often lack important features provided by integrated app store billing (unified subscription management / parental controls etc.)
- Three out of four developers say users may find it confusing to manage subscriptions or get support when billing is handled through alternative services.
- 73% say users are likely not to trust alternative billing services with their payment information.
- 70% said they are concerned about their company's ability to effectively manage fraud and security risks when using alternative billing services.

E. **There is no demonstrated consumer harm that warrants additional steering intervention**

A study by Professor Fradkin and Dr. Burley of the Analysis Group highlights how developers on the app store have more ways than ever to monetize their apps. Apple's app store, for example, is a trillion-dollar economic engine for app developers. The study found that in 2024, Apple's global app store helped developers achieve $1.3 trillion in sales and billings. Within Europe, the UK had the largest amount of billings and sales facilitated by the App Store ecosystem — with $55.1 billion in estimated UK billings and sales facilitated by the App Store ecosystem in 2024. These developer revenues fuel local businesses, enable competition, and help support the creation of entirely new kinds of apps that improve people's lives and create new business opportunities.

The debates around payment steering relate to a very small portion of total billings and sales — just 3% — that Apple earns on digital goods and services transactions — with 97% accruing to developers without any commission owed to Apple.

While the solicitation posits that a steering intervention to promote alternative ways to transact outside of the app, thus avoiding commission fees, "could have significant benefits for UK mobile users and app developers as well for businesses across the economy more widely," such an intervention is more likely to introduce serious new harms, without lowering costs for consumers or enabling new competition.

Link-Outs

We understand CMA's focus and questions on steering to be targeted at link-outs (actionable links that take users outside the app to complete a transaction) as a means for enabling competition by allowing more transactions outside of the integrated billing system. However, as we have seen elsewhere, such interventions create new consumer complexity, duplicative functionality, and introduce new privacy, safety and security issues without creating new competition, enabling consumer savings, or addressing any specific consumer harm. Link-outs to external websites are a well-known exploitable security vulnerability — especially when they link to unvetted, unverified websites that don't belong to the app developer itself.

We are glad to see that CMA recognizes that such a steering intervention can create new harms, for example, "the potential for lower security and privacy protections, or the loss of centralised billing and management)." (Paragraph 11(b) of the solicitation)

We think CMA has identified some of the relevant concerns, and we want to explain these in more detail, and highlight lessons from relevant international interventions below.

F. Europe's DMA link-out strategy highlights critical privacy, safety and security risks for users.

One of the major digital disconnects in the EU's Digital Markets Act (DMA) rules involve Article 5(4) which requires gatekeepers to allow apps to "steer" users using "link-outs" to external web links to allow business to communicate, promote and use alternative payment mechanisms. In this provision, regulators singled out Apple. Despite the fact that Apple already met the 5(4) obligations of allowing developers to communicate and promote offers for purchase of digital goods at a destination of the developers' choice, in April 2025, the European Commission fined Apple €500 million seeking to drive changes that might benefit a few large developers, at the expense of weakening the privacy, safety and security safeguards for large numbers of users.

For example, in accordance with 5(4), developers on Apple's platform can communicate and promote offers for purchase of digital goods at a destination of the developers' choice. This can include information about subscription pricing or other offers available within or outside the app, and can provide instructions for how to subscribe to offers outside the app. But regulators chose to apply hefty fines for Apple's attempts to balance these mandates with efforts to protect consumer privacy and security — safeguards that are consistent with privacy requirements under Europe's GDPR and security requirements under Europe's CRA. In Apple's case the EC attempted to prioritize benefits to a few large app developers by weakening consumer privacy and security protections for millions — protections that are well known and broadly used throughout the digital ecosystem to keep users safe.

Link-outs to external websites are a known exploitable vulnerability

Mandating unrestricted link-outs can enable threat actors to harness these links to distribute malicious apps, hijack accounts via fake login pages, expose users to fraudulent scams, or deploy

spyware undetected. The open web is a well known hotbed for criminals, scammers and fraudsters. Regulators must always think about the reality of today's online ecosystem — that not everyone is a good actor, or has the consumer's welfare at heart.

The UK's National Cyber Security Centre, for example, has developed extensive resources to "watch out for suspicious links." They say, "Cyber criminals insert malicious links into SMS text messages, emails, and increasingly on social media posts." CMA shouldn't expand this list by also including apps to the list of places where criminals insert malicious links. Why does the NCSC warn about these harms? Because there is already a multibillion industry aimed at tricking people into clicking on things they shouldn't. According to the FBI's Cybercrime report, the number one reported cybercrime involved efforts to get people to click on a legitimate looking but malicious link or URL. Zimperium found that 82% of all phishing sites now target mobile devices. But under the DMA, platforms are being restricted from comprehensively protecting users from scammy and malicious link-outs.

According to the UK's Cyber Security Breaches Survey 2025, 85% of businesses experienced a breach or attack in the last 12 months with phishing attacks remaining the most prevalent and disruptive type of breach or attack — efforts to trick users into clicking onto a link that they shouldn't.

Within the UK alone, the government has helped block almost 1 billion attempts to access malicious websites. Given the breadth and prevalence of efforts to get UK consumers to click on untrusted links, the government should be equally concerned that bad actors would try to leverage untrustworthy links in apps too.

Allowing link-out URL redirects is a known exploitable vulnerability. URLs are not always born malicious. They can become weaponized post-delivery. One common vulnerability involves redirects — which can obfuscate where the link is actually taking the user. These create several types of risks. For example, a malicious actor could release an app that appears to be a legitimate app but uses external links to redirect users to a malicious alternative payment site aimed at stealing credit card or login credentials. App stores can and do play important roles in vetting apps for various kinds of risks like this.

There are also redirects that are used to get around popular and common consumer privacy protections built into smartphones aimed at preventing activity from being tracked across apps and websites like "Ask App Not To Track" or third-party cookie blocking. Tracker redirects get around these privacy protections by momentarily (and imperceptibly) redirecting a user to the trackers website to use first-party storage to track that user across websites. Some major browsers include features to protect against these kinds of anti-privacy tactics by blocking third-party cookies that can track users across sites and apps to create digital dossiers and target ads. Apple's Safari Intelligent Tracking Prevention for example has sophisticated built-in technologies to help prevent redirect privacy weaknesses and avoid cross-site tracking capabilities. But the ability to track a user's online activity by avoiding built in features designed

to prevent user activity tracking, can be extraordinarily lucrative for companies who have built their business on hoovering up and private details about a user's online activities.

Information exposure through link-out URL parameters passing is a known exploitable vulnerability

Another significant privacy and security risk contemplated by the DMA involves requiring mobile platforms to allow link-out URLs to include passed parameters information. The DMA's "Link-out" requirements create additional security inconsistencies, and allow URLs to include passed parameters which can be used to pass personal and sensitive information. URL parameter passing is a significant privacy and security risk as it can expose sensitive information including PII, user identities, session tokens, API keys, or any other data stored on a phone. These are known exploitable vulnerabilities. DMA regulators are requiring smartphones to allow external links that contain any amount of PII and other information to be transferred outside of the EU to any external website in any country, even to a website that doesn't even belong to the app developer. Regulators are requiring this despite the fact that Europe's flagship privacy law GDPR imposes restrictions on the transfer of personal data outside the European region.

To protect users, some browsers, like Safari, strip out known tracking parameters from URLs But there are big companies with major apps built on a business model based on hoovering up as much private information as possible. They use tricky tactics in order to add additional parameters to URLs and get around efforts to protect privacy. Everyone's privacy should be protected, but these DMA mandates inappropriately restrict it.

G. Link-out provisions can undermine efforts to block scams and fraud

The UK is already a hotbed for online consumer scams and frauds. According to Stop Scams UK, fraud accounts for 41% of all crime in England and Wales. UK Finance reported that criminals stole a staggering £629.3m through scams and payment fraud, with two-thirds of all fraud beginning online, in the first half of 2025. The UK's **Stop! Think Fraud** campaign tells us that criminals use a wide range of methods and tactics to steal your money.

Mobile app marketplaces and their accompanying robust governance mechanisms have long gone to extraordinary lengths to fight against fraud and scams on their platforms, and to prevent efforts to trick people via scams to make fraudulent transactions. For example, in the last 5 years, according to Apple's annual App Store fraud analysis, its App Store has protected users by preventing over $9 billion in fraudulent transactions, including over $2 billion in 2024 alone, Likewise, Google's Play Store app marketplace governance mechanism prevented over $2 billion in fraudulent and abusive transactions in 2022.

One of the key ways that existing app governance models have sought to prevent and deter fraud is to protect users from scammy and malicious links that take users outside of the trusted app marketplace environment in direct them to a legitimate looking but fraudulent/malware laces website in order to steal personal information like banking credentials. But the DMA weakens

the safeguards designed to protect consumers, expanding opportunities for fraudsters to take advantage of the Internet's dark side.

A recent UK Consumer Security Survey on mobile app security finds high consumer interest:

- 62% of UK consumers declared mobile fraud their number one concern
- 80% favour pre-emptive anti-fraud measures
- 27% report first-hand experience or second-hand awareness of social engineering scams
- 56% of people in the UK now prefer using mobile apps over other channels to buy goods and services
- 97% of UK consumers now believe that protecting their privacy when using mobile apps is essential
- The number of UK consumers who fear "developers don't care" about protecting the mobile app has increased by 171%.

The CMA should continue to support these consumers, and their interest is making secure mobile payments without weakening privacy, safety or security protections built into integrated payment systems.

H. Link-Outs can undermine a parent's ability to protect their children.

As CMA noted in its solicitation for comments, link-outs can undermine existing guardrails around centralized billing and management. One especially important loss for consumers involves popular parental control tools. As we saw in Europe's DMA implementation, "link-out" requirements also weaken a parent's ability to use popular app store based parental control tools like Report a Problem, Family Sharing, and Ask to Buy — which will not reflect the in-app "link out" transactions. Apple's "Ask To Buy" feature, for example, allows parents to decide which apps their kids download from the App Store, lets parents approve their children's in-app purchases, and provides confidence that scammers and abusive actors are not targeting their children.

The ability to restrict in-app purchases has been an especially important feature for UK parents going back years. In 2013, for example, before these key app purchase features were integrated into app stores, two parents managed to get a refund after their son spent £980 buying virtual donuts in a Simpson's game, while another eight-year-old girl ran up a bill of £4,000 from games such as My Horse and Smurfs' Village. To respond to these and other challenges, app marketplaces have incorporated important safeguards that for example enable parents to turn off in-app purchases entirely, or they can use an "Ask to Buy" feature to control in-app purchase. If they let children use their devices, they can require a password for every purchase. Our own Trusted Future survey found parents strongly support the parental safety tools that smartphone makers have built into their mobile device app stores, including 88% who support a gatekeeper's ability to restrict children's in-app purchases. CMA should not break the trust that parents have in these tools.

It's not surprising that some one of the world's largest game developers is one of the loudest proponents of anti-steering link out provisions. Video games are some of the most lucrative apps in the mobile ecosystem — making up approximately 51% of total game revenue worldwide. These mobile games rely heavily upon a free-to-play model which depends on in-app purchases for games that are free to download — a business model that European Consumer Organization BEUC calls "manipulative."

It's such a lucrative market that it should be no surprise the biggest companies behind some of the biggest online games have sought to maximize revenue by manipulating and tricking children into making in-app purchases that their parents may not approve of. It's the kind of activity that led the US Federal Trade Commission (FTC) to fine Epic Games $245 million in 2023 for tricking children into racking up in-game charges without any parental involvement — which was the FTC's largest administrative order in history. Similarly in May of 2024, the Netherlands' Authority for Consumers and Markets fined Epic Games €1.1 million for its "pressure selling tactics" urging kids to make in-app purchases in its children's targeted Fortnite game. In no case should CMA take steps to undermine a parent's ability to manage and prevent their children's in-app purchases — undermining trust in the platform.

I. Link-Outs don't foster new competition.

Proponents of steering and link-out intervention often say they are necessary to promote greater competition. However, evidence from the EU's DMA interventions did not spur European startup creation or growth and may have harmed the entrepreneurs it was supposed to help. An economic analysis by CCIA found that:

- **VC investment in startups declined after DMA implementation**. European venture capital investment fell 37% from 2022 to 2024 even as global stock markets rose 40%.
- **IPOs did not increase.** The data show no increase in European IPOs post-DMA. IPOs were just 6% of exits, and most startups are far too small to IPO successfully.
- **The DMA eliminated acquisitions by targeted companies.** The seven companies targeted as "gatekeepers" under the DMA made zero acquisitions of European venture-funded startups in 2023 and 2024, a sharp drop from years prior to the DMA.

However, the existing app marketplace and all that comes with it is a proven enabler of competition and small business growth. For proof that app marketplaces enable small startups to become global powerhouses, look to the example of Spotify's digital market. Starting out as a small startup in Sweden, Spotify has grown their company into the largest digital music streaming business in the world. Spotify now has almost half of the UK's music streaming market — more than double their closest competitors.

A large part of Spotify's success is due to access to the two primary app marketplaces, along with all the tools and technology that Spotify uses to build, update, and share their app with mobile users around the world. Yet they pay neither Apple nor Google for the access and

services that have helped make them a leading music service and one of most recognizable brands in the world. The Spotify app has been downloaded, redownloaded, or updated more than 119 billion times on Apple devices, and is available in over 160 countries spanning the globe.

Spotify continues to enjoy staggering growth rates in an obviously thriving market — despite claiming that competition is being stifled by high commission rates. Spotify, for example, has paid Apple nothing, zero commissions for access to its global app marketplace, and yet in 2024 earned net profit of €1.1 billion thanks in large part to access to the mobile ecosystem. Spotify has gotten a free-ride — able to take advantage of substantial investments in payment processing systems, in the development of a trusted global market app distribution system, a system for app discovery, app marketing tools, app analytics, and app APIs.

Nonetheless, Spotify has been a loud voice in seeking app store regulatory changes to gain even more market advantages — changes that allow them to further cement their dominant position in the market and further consolidate the music streaming market. But these changes are unnecessary for enabling new entrants, are not supported by the evidence, and as we have described can create new consumer harms that undermine trust.

Most apps, and especially new entrants, benefit from having a built-in trusted payments system that they don't have to build themselves — including the refund systems, the ability to handle local issues like taxes, and other features. Because only larger apps have the resources to create their own payment system that works globally, such a proposal is likely to disproportionately benefit larger apps at the expense of smaller app developers. App stores are the only place where small app developers are on an equal footing with large developers. For these reasons, it's clear that the UK doesn't need novel steering remedies — especially based on competition grounds.

J. An intervention to lower commission fees does not lower app prices or create consumer savings.

Europe's DMA also provides key lessons for how well-intentioned efforts aimed at improving competition (for example around steering) did not have the intended effects. For example, one of the expected benefits of the DMA was around reduced commissions on app stores. But the actual market effects have been underwhelming. The European Commission believed that if developers pay reduced fees, those savings will be passed on to consumers through lower prices. But a study by Analysis Group suggests that lower commission fees have not led to lower app store prices. The study looked at 41 million app store transactions across 21,000 paid apps and in-app purchases, comparing app prices for three months before developers enrolled in the alternative business terms to prices for three months after they enrolled. 91 percent of the time, prices did not go down, even though fees dropped by 10 percentage points on average. In some cases, developers raised their prices. As reported:

- *"The top five EU app developers did not change their app pricing despite the reduced commission, instead keeping the additional revenue. Developers paid an estimated 20.1*

million euros less in commission fees to Apple after the change. More than 86 percent of the savings went to developers outside of the European Union.

- *When developers did lower prices, the average decrease was 2.5 percent, seemingly unrelated to the DMA. Apple says that it saw the same effect when it launched the App Store Small Business Program. The lowered fees did not result in meaningful savings for consumers because only a small minority of developers decreased their prices.*
- *The study says that the percentage of fee reductions does not change over a longer eight-month period, and that the Core Technology Fee paid by apps with more than one million first-time installs per year also does not change the results. 80 percent of the apps in the study did not pay the CTF."*

By contrast, commissions can finance platform investments that benefit both users and developers. These fees can help support security, user experience, and anti-fraud protections that help foster the trust necessary for users to rely on the platform, thereby expanding the potential audience for developers. In this way, it helps strengthen network effects, increasing a platform's value as participation grows.

K. Static text is a safer alternative to active link-outs.

The solicitation contains insufficient details on what specific steering proposals the CMA may be considering — and details matter. Given the preponderance of evidence discussed above, about the fundamental challenges involved in allowing untrusted active link-outs to external payment systems, we would encourage CMA to pursue other means to achieve its goals. If it determines that consumers need better information on ways to take advantage of better deals outside of app stores, it can instead evaluate the use of a static text banner. Static text can make users aware of better deals without creating new user privacy and security risks, or undermining trust.

L. How Japan addressed some of the most significant privacy, security and child safety weaknesses inherent in Europe's approach.

Japan's Mobile Software Competition Act (MSCA) entered into force on December 18, 2025. The Act requires Apple and Google, as operators of smartphone platforms and ecosystems, to open their systems with the goal of fostering competition. While far from perfect or ideal, we can already see that Japan's more pragmatic approach to preserving key guardrails in its approach to its Mobile Software Competition Act (MSCA) is far superior to Europe's failed DMA approach.

While Japan's MSCA will still lead to an increase in privacy, safety and security risks, its regulators have nonetheless done a better job of acknowledging and addressing some of the most significant privacy, security and child safety weaknesses inherent in Europe's approach. For example, Japan has more explicitly written in a set of more appropriate guardrails which will lead to better solutions for protecting Japan's consumers and businesses. Japan's approach helps

better protect children and empower parents by ensuring consistent age ratings and protections for children. And they've enabled payment choices that put trusted choices side by side with other alternatives.

> **Child Safety.** Unlike Europe, Japanese regulators have enabled key guardrails to better protect its kids. For example, Japan explicitly allows companies to take steps "safeguarding youth who use smartphones" — including "measures to establish parental functions in the basic operation software." In practice, this means apps in the app store's children's category for users under 13, can't include external transaction link-outs. This protection, not allowed in Europe, means that Japanese children are more protected from scams, and parents have better controls.
>
> **Side by Side Payment Options.** Unlike Europe, Japan's MSCA enables developers to offer third-party payment options or links to external sites for purchases but does so in a way that puts trusted choices side by side with other alternatives. While still creating new risks, it nonetheless gives consumers the ability to choose the approach that they feel they can trust, and that best meets their needs. Likewise, unlike Europe, when users choose an alternative system, they are kept informed when they are not transacting with the phone's built-in payment system and can be warned that the ability to obtain a refund from the phone's system is no longer available for outside payments. This is a significant improvement to Europe's DMA approach that specifically prevented privacy and security safeguards from being implemented as a part of the alternative payment link-outs – and required known security vulnerabilities and privacy weaknesses to be built into alternative payment requirements.

In sum, Japan's approach takes a more realistic view of our digital world than does Europe. It recognizes that the digital world has bad actors, it better understands the critical role that app stores play in reviewing and protecting users, and it listened to experts in choosing not to replicate the most egregious harm caused by Europe's failed DMA approach.

Conclusion

Trusted Future welcomes this opportunity to contribute to the CMA's call for evidence. We hope the CMA will use this opportunity to take an evidence-based approach that continues to support the essential elements necessary for driving trust throughout the mobile ecosystem by ensuring any changes ensure privacy, safety, and security measures remain a core priority.