DMA IMPLEMENTATION WORKSHOP ON APP STORES — HARD TO SQUARE THE CIRCLE

The European Commission is moving forward on its implementation of the recently passed Digital Markets Act (DMA). To this end, it is holding a series of public workshops to discuss difficult implementation issues. On Monday, March 6th the Commission is holding a workshop on the app store provisions of the DMA. The app store provisions seek to force smartphone producers to allow any app to be downloaded onto a smartphone, regardless of whether it has been checked for security or privacy issues, or subject to official app store rules and official app store required lifecycle maintenance.

Given the state of cybersecurity today, and the activity of cyber criminals, nation-state actors, and privacy abusers, there is significant concern that forcing mobile device producers to 'open-up' their device to any and every app will predictably lead to significant cyber risk and loss for consumers, enterprises, critical infrastructure, and government networks and data, all of which use the devices that will now be subject to the DMA app store provisions. These safety, security, and privacy issues were discussed during passage of the DMA, and now the Commission is holding a workshop to understand the implications.

The safety, security, and privacy issues are recognized within the DMA itself, where the section on forcing the allowance of every and any unvetted app or unvetted app store onto devices also says that the device producer also must be able to ensure the security and integrity of the device and the security of the device user. These are in direct tension, and seemingly in direct conflict.

Implicitly, the DMA recognizes that it is not possible to force unvetted apps onto devices and have security today, as the recitals to the relevant sections say 'it should be possible' to allow unvetted apps onto the device and ensure security, without reciting how that's possible, or stating that it is possible. It is a statement about an unknown future hoped-for state. There is no evidence that such a state exists, or that it could.

The DMA also states that providers have to be able to comply with other applicable laws, and again there is tension, and conflict, with existing and proposed EU privacy and security laws such as the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the proposed Cyber Resilience Act (CRA). Finally, the DMA states that the Commission can exempt a provider from the obligations of the DMA where required for public security, and one has to ask whether that exemption should apply to the forcing of unvetted apps onto a device given the significant national security concerns that Member States will have with the introduction of vulnerabilities onto devices used in critical infrastructure, military, and intelligence networks, and the ability to spread disinformation through unvetted apps, and inability to remove apps spreading illegal content,

during growing geopolitical tensions, Russia's invasion of Ukraine, and upcoming elections. This analysis explores some of the challenges, internal cross purposes, and questions created by the DMA as it relates to the app store provisions examined at the Workshop.

This analysis also sets out lessons to be learned by the DMA experience for policymakers in Washington who have considered, and so far rejected, provisions similar to the DMA.

This analysis finds:

- DMA provisions to force the use of apps not from official app stores onto devices, and allow such apps interoperability with device technologies, run counter to government security agency suggested best practices for protecting the security and privacy of mobile device users.
- It seems impossible to square the circle between allowing any and every unvetted app onto devices and maintaining or ensuring the security and privacy of consumer, enterprise, critical infrastructure, and government users, networks, and data.
- The DMA requirement to comply with other security and privacy laws such as the GDPR, DSA, and pending CRA, will create conflict with the unvetted app requirements of the DMA, making it even harder hard to square the circle on how to comply and maintain security, privacy, and police disinformation and illegal content.
- The exemption from obligations of the DMA due to public security, would seem to apply to the increased cyber risk from the app provisions, and the Commission and Member States (which retain 'competency' for national security) could find that the predictable adverse impact on consumer, enterprise, critical infrastructure, military, and intelligence networks and data leads them to a finding that an exemption from compliance, at least until the security of the European Union and all Member States can be ensured, is warranted.

1. INTRODUCTION

Regulation 2022/1925, or as it is more commonly referred to as the Digital Markets Act, is a European Union regulation with the objective of restructuring the digital marketplace in Europe. It was first proposed by the European Commission in December 2020, was signed into law by the European Parliament and the Council of the EU in September 2022, and went into effect on November 1, 2022, and will become applicable on May 2, 2023.

The DMA applies to large online platforms, defined as "Gatekeepers," and consists of a series of prohibitions and requirements, "do's and don'ts." The focus of the March 6 European Commission Workshop will be on "The DMA and app store related provisions."

The terms of the DMA app store provisions affect highly technical technology and content ecosystems, and must be reconciled with the limits and principles of hardware and software systems engineering, and the realities of the hotly contested global cyber security environment. In this analysis we look at the sections pertinent to app stores, set out what the DMA appears to require, the existing best practices in those areas, and ask questions that may be relevant about how the Commission and Member States think about implementing often countervailing requirements, interests, and values. We are pleased that the European Commission is holding this Workshop to grapple with these critical and impactful issues and questions.

2. DMA ARTICLE 6(4): INSTALLATION AND EFFECTIVE USE OF THIRD–PARTY SOFTWARE APPLICATIONS OR SOFTWARE APPLICATION STORES.

Article 6.4 of the DMA has two parts, the obligation to allow any and every app or app store to be installed on a device, and the countervailing recognition that the security and integrity of the device and of the user (consumer, enterprise, critical infrastructure, military, intelligence) must be maintained.

The first part of Article 6.4 of the DMA deals with forcing any and all apps onto devices, stating:

> "[the] gatekeeper shall allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that gatekeeper."

And the second part of Article 6.4 recognizes the need for security and integrity of the device and users, stating:

> "[the] gatekeeper shall not be prevented from taking…measures to ensure that third-party software applications or software application stores do not endanger the integrity of the hardware or operating system…." and "the gatekeeper shall not be prevented from applying…measures and settings other than default settings, enabling end users to effectively protect security in relation to third-party software applications or software application stores."

Currently, device producers create combinations of hardware and software protections that are integrated and designed to 'build security in' from the start, using systems engineering within the device, requirements in app stores that apps pass machine and human security checks before being available to be downloaded onto the device, require that app developers state their privacy policies and adhere to them, and require and manage patching of vulnerabilities in apps by a secure methodology. They also constantly improve the security protections of the software, hardware, and apps as the global cyber threat environment morphs over time. Net-net, to protect devices and users, apps are vetted before they are used in consumer, enterprise, critical infrastructure, or government networks. Importantly, device makers sell, and users use, the same device in all of these networks – from consumer to military – and if Article 6.4 forces a change in the security architecture of the system, it's forced across all uses, even those run and maintained by Member States for national security networks.

App developers create millions of apps across the globe. Only a portion of those apps meet the official app store requirements for safety, security, and privacy. Currently, app stores reject hundreds of thousands of apps a year because of non-trivial security and privacy issues. Criminals and nation-state actors attempt to find ways to trick users into downloading their unofficial apps onto user devices. As app creation is a global phenomenon, apps

can originate from all over the world, including places known to use cyber means for theft, fraud, disinformation, vandalism, terrorism, espionage, and war. The mobile phone has access to some of our most sensitive data and are also often used in businesses and critical infrastructure operations under enterprise Bring Your Own Device (BYOD) policies. Our lives and our businesses are on or mobile devices. Criminals and nation-states will likely welcome any rule changes, like Article 6.4, that force device producers to allow any app from anywhere to be downloaded onto the devices and interoperate with the software and hardware of the device. It opens-up the attack surface.

Device producers engineer their software and hardware to provide security defense in depth of the device and data. Access to software and hardware elements in devices are highly constrained. An even more constrained number of highly trusted and controlled, and device producer created, applications are ever allowed to access lower-level elements of the device. For example, unlike other devices, full read and write access to the hard drive is commonly restricted on smartphones which has the beneficial effect of preventing ransomware attacks that abuse lower-level access to encrypt a hard drive in its entirety in exchange for a ransom payment. To the extent Article 6.4 or Article 6.7 (Providing Interoperability to Hardware and Software Features) forces the requirement that non-official app store apps must be able to interoperate with device software or hardware, these provisions would be granting access, or a toehold, onto the device and opening the door for non-vetted apps and actors to execute maligned activity on the device. In security, the adversary attempts to get into a network or device in the simplest way possible, and once they have established a toehold, move laterally, and deeper into the most sensitive areas of the network or device to steal, surveille, degrade, or destroy the data or device. Granting interoperability to millions of unknown, untrusted, or unvetted apps or updates would further erode security and privacy.

Currently, the official app stores of the 'gatekeepers' undertake security and privacy reviews and keep out these security and privacy risks. They also remove apps that violate the law, or the device terms of service, or fail to follow the security or privacy promises the app made to gain access to the official app store. They require patching, and secure delivery of patches. All these activities are vital to creating a safe and secure environment for the user. Further, the current app stores of the 'gatekeepers' have an incentive to run effective safe and secure app stores – the usefulness and trustworthiness of their devices is squarely at issue, as is their interest in a safe mobile device ecosystem. No one has a stronger incentive to ensure a safe and secure environment.

The risk of apps from outside the official app stores is a well-known problem, and one recognized by the security and privacy agencies around the world. It is simply a best practice to only use the official app stores, and not to download apps from other places. This includes guidance from:

- **The European Union Agency for Cybersecurity (ENISA):** in its August 24, 2016, publication "Vulnerabilities – Separating Reality from Hype" recommended that people "Use the official application marketplace only... to minimize the risk of installing a malicious application. Users should not sideload applications if they do not originate from a legitimate and authentic source."

- **The European Union Agency for Law Enforcement Cooperation (Europol)** advises mobile device users to "Only install apps from official app stores... Be cautious of links you receive in email and text messages that might trick you into installing apps from third party or unknown sources."

- **The U.S. National Security Agency:** "Install a minimal number of applications and only ones from official application stores."

- **The U.S. Federal Trade Commission:** "Use official app stores. To reduce the risk of installing potentially harmful apps, download apps only from official app stores, such as your device's manufacturer or operating system app store."

- **The UK's National Cyber Security Centre:** "Only download apps for smartphones and tablets from official stores (like Google Play or the App Store). Apps downloaded from official stores have been checked to provide protection from viruses and malware."

- **India's Ministry of Electronics and Information Technology's Computer Emergency Response Team (CERT-In):** "Reduce the risk of downloading potentially harmful apps by limiting your download sources to official app stores, such as your device's manufacturer or operating system app store. Do not download from unknown sources or install untrusted enterprise certificates. Apps that are available from 3rd party sellers may not be legitimate and could contain malwares."

- **And other agencies globally.** [i] *see footnote 1.

Opening-up the door to millions of unvetted apps raises the issues these security and privacy agencies warn against. The 'gatekeeper' device companies have built up layered defense-in-depth systems, that constantly adjust to keep up with the advancing cyber threat and keep devices and users safe and secure. A central part of that is the machine and human vetting, secure updating, privacy and data use transparency, and when necessary, removing apps. It's hard to square the circle about how devices and users will be safe and secure without these practices.

QUESTIONS FOR POLICYMAKERS:

- Given that Article 6.4 may be deemed to open-up the device to any and every app, how will the Commission and device producers protect the security and privacy of users?

- The official app stores use machine and human review of app security, require data use transparency, adherence to security and privacy law, require and securely deliver patches for vulnerabilities, reject hundreds of thousands of apps for security and privacy deficiency and create and maintain a safe mobile ecosystem – who, and how, will that be accomplished if the device producers cannot ensure the safety, security, and privacy of the apps?

- How does the Commission assure EU citizens, businesses, and Member State national security agencies that the Commission's implementation of Article 6.4 will not make them less secure, lessen privacy, or open the door to maligned actors to spread disinformation, insert spyware, steal data, or brick their devices?

- How does the Commission square the circle between the two directions of Article 6.4 – opening-up the device to millions of unvetted apps and ensuring security of the device and user?

- How does the Commission view the best practice recommendations of ENISA, Europol, NSA, FTC, FBI, NIST, UK NCSC, India CERT, and other agencies only to download apps vetted by official app stores?

- If device makers can't use a full range of defense-in-depth mechanisms to drive innovation and security into their devices, why won't that turn the clock back on decades of cyber policy, where government leaders urge companies to 'bake' security into products? Or make products secure by design? Or make products secure by default? Aren't all these practices advocated by the Commission and Member States?

- If the Commission grants technical interoperability on devices to unknown apps, how can the Commission assure consumers, critical infrastructure owners, Member State governments that they are not creating a toehold for malign actors and action, not forcing negative changes in the security architecture of the device, or forcing the device to be less effective or integrated? Isn't this problem even worse if device producers have to grant the same level of access to untrusted apps that they grant to their own specially engineered apps providing similar services?

3. DMA ARTICLE 8: COMPLIANCE WITH OBLIGATIONS OF GATEKEEPERS

Article 8 also requires that covered companies are both in compliance of both the DMA and other applicable EU cybersecurity, consumer protection, and product safety laws. Article 8.1 states:

> "The gatekeeper shall ensure and demonstrate compliance with the obligations laid down in Articles 5, 6 and 7 of this Regulation. The measures implemented by the gatekeeper to ensure compliance with those Articles shall be effective in achieving the objectives of this Regulation and of the relevant obligation. The gatekeeper shall ensure that the implementation of those measures complies with applicable law, in particular Regulation (EU) 2016/679, Directive 2002/58/EC, legislation on cyber security, consumer protection, product safety, as well as with the accessibility requirements."

A number of existing, and pending laws are implicated, including the General Data Protection Regulation (GDPR), Digital Services Act (DSA), and the pending Cyber Resilience Act (CRA). All of these have provisions which would be adversely affected by the app store provisions of the DMA.

Under the GDPR, personal information controllers and processors have obligations to obtain consent for the collection, use, and transfer of personal information, as well as obligations to protect the data. Currently, the official app stores require that app providers state the terms of their use of the data collected, maintain the security of the app, and comply with applicable law. To the extent these obligations are not faithfully executed, they have to cure any deficiency, or potentially be removed for the official store. If device producers are forced to allow any and every app or app store onto the device, the apps from other than the official app store will carry none of these protections, including compliance with the obligations under the GDPR.

Under the new DSA, Section 5, Article 33 and 34, Very Large Online Platforms and Very Large Online Search Engines have obligations with regard to the dissemination of illegal content, negative effects for the exercise of fundamental rights, negative effects on civil discourse and electoral processes and public security, as well as mitigation responsibilities. As with the GDPR, the official app stores of device producers vet apps for compliance with safety, security, and privacy obligations and terms and conditions, and such vetting and ability to uphold obligations that exist with the use of the official app store would not exist for apps that device producers were forced to allow on their devices without the safety, security, and privacy requirements of the app stores.

The pending CRA may be the hardest to comply with to the extent the DMA forces unvetted apps onto devices. The CRA was introduced by European officials stating the critical nature of device and product security in the EU given the nature of cybersecurity threats to EU consumers, enterprises, critical infrastructure, and government networks and data.

In releasing the CRA officials stated (emphasis added):

> "We deserve to feel safe with the products we buy in the single market. Just as we can trust a toy or a fridge with a CE marking, the Cyber Resilience Act will ensure the connected objects and software we buy comply with strong cybersecurity safeguards. It will put the responsibility where it belongs, with those that place the products on the market."
>
> **Margrethe Vestager, Executive Vice-President for a Europe Fit for the Digital Age**
>
> "The Cyber Resilience Act is our answer to modern security threats that are now omnipresent through our digital society. The EU has pioneered in creating a cybersecurity ecosystem through rules on critical infrastructure, cybersecurity preparedness and response, and the certification of cybersecurity products. Today, we are completing this ecosystem through an Act that brings security in everyone's home, in all our businesses and in every product that is interconnected. Cybersecurity is a matter for society, no longer an industry affair."
>
> **Margaritis Schinas, Vice-President for Promoting our European Way of Life**
>
> "When it comes to cybersecurity, Europe is only as strong as its weakest link: be it a vulnerable Member State, or an unsafe product along the supply chain. Computers, phones (emphasis added), household appliances, virtual assistance devices, cars, toys… each and every one of these hundreds of million connected products is a potential entry point for a cyberattack. And yet, today most of the hardware and software products are not subject to any cyber security obligations. By introducing cybersecurity by design, the Cyber Resilience Act will help protect Europe's economy and our collective security."
>
> **Thierry Breton, Commissioner for the Internal Market**

The CRA will require mobile operating system producers to ensure security by default (whereas DMA Article 6.4 forbids default configurations to protect the security and integrity of devices and users); ensure no unauthorized access (whereas DMA removes the device producers from ensuring safety, security and privacy of apps); protect confidentiality of data (whereas DMA removes device producers' ability to hold apps to stated privacy promises); "be designed, developed and produced to limit attack surfaces, including external interfaces" (whereas the DMA requires unvetted apps which expand the attack surface and unvetted external interfaces); and ensure that security patches are disseminated without delay (whereas if apps are not from the official app store, the device producer cannot ensure essential patches are ever delivered and applied).

The requirements of the DMA, that ban default security configurations, force device producers to allow millions of apps that have not been vetted, grant interoperability to untrustworthy software, and divorce apps on devices from safety, security, and privacy requirements, run counter to what will be required by the CRA. Another place where it is hard to square the security circle.

QUESTIONS FOR POLICYMAKERS:

- What is the effect on GDPR compliance by app developers when they don't go through the official app store? What is the effect on the privacy of EU citizens?
- What is the effect on the ability to ensure compliance with the DSA when apps, with large and small numbers of EU users, would no longer go through the official app store?
- How can a mobile operating system producer (mobile device producer) comply with the proposed CRA when the CRA and DMA requirements conflict?
- Given the top importance to cyber security indicated by EU leadership, and the apparent conflict between the DMA and the CRA, which law should device producers comply with, and who will decide?

4. DMA ARTICLE 10: EXEMPTION FOR GROUNDS OF PUBLIC HEALTH AND PUBLIC SECURITY

Article 8 also requires that covered companies are both in compliance of both the DMA and other applicable EU cybersecurity, consumer protection, and product safety laws. Article 8.1 states:

> "The Commission may, acting on a reasoned request by a gatekeeper or on its own initiative, adopt an implementing act setting out its decision, to exempt that gatekeeper, in whole or in part, from a specific obligation laid down in Article 5, 6 or 7... where such exemption is justified on the grounds... of public health or public security."

In 2019, NATO Secretary General Jens Stoltenberg stated that "cyber defences and resilience will be a top priority," noting that "cyber-attacks can be as damaging as conventional attacks... [and] are becoming more frequent, more complex and more destructive." This was before Russia's 2022 invasion of Ukraine, and the use of cyber as a military tool 'blended' with kinetic attack. In 2018 the United States Director of National Intelligence first placed the cyber threat at the top of the list of worldwide threats. The 2022 United States Worldwide Threat Assessment (WTA) continues to highlight the cyber threat, listing state actors including China, Russia, Iran, and North Korea. The Assessment specifically cites national security risks to critical infrastructure, private sector networks, and its use as a military tool. The WTA further observes that, "Transnational cyber criminals are increasing the number, scale, and sophistication of ransomware attacks, fueling a virtual ecosystem that threatens to cause greater disruptions of critical services worldwide." And as we've seen, disinformation – delivered by apps – is rampant in elections, COVID and Russia's invasion of Ukraine. Forcing apps that spread disinformation onto devices, not subject to app store rules or removal, is a national security issue too.

This is no time to introduce cyber vulnerabilities or disinformation into EU consumer, enterprise, critical infrastructure, military or intelligence networks and data. In commercial products generally, and in the mobile devices subject to the DMA, the same mobile devices are used in all consumer, critical industry, and government networks. In technology issues, Member States retain 'competency' over national security issues, and the EU is granted competency over non-national security issues – both are critically important, and both are implicated by the predictable lessening of public security and safety pursuant to the app store provisions of the DMA. Given the state of cybersecurity in both spheres, it is an Article 10 'public security' issue.

The Workshop is asking for feedback on the implementation of the app store provisions. As discussed earlier in this analysis, it is hard to square the circle of how one could allow millions of apps not subject to the official app store onto a device and maintain security in consumer, enterprise, critical infrastructure, military, and intelligence networks. Perhaps until that circle can be squared device makers should be exempted from application of Article 6.4 pursuant to Article 10.

QUESTIONS FOR POLICYMAKERS:

- Given the national security and commercial cyber security and disinformation risks of associated with DMA Article 6.4, isn't Article 10 public security implicated?

- If Article 10 is implicated, should the application of Article 6.4 be exempted until the Commission and Member States and stakeholders (device producers and consumer, enterprise, critical infrastructure, military, and intelligence network and data owners and operators) are satisfied that Article 6.4 can ensure security now and into the future?

5. LESSONS LEARNED — US POLICYMAKERS

So far, U.S. policymakers have considered and rejected DMA like economic regulation. As this analysis has indicated, forcing device producers to allow millions of apps onto the device that are not from the official app store will raise significant national, commercial, and consumer security and privacy issues. Given the intensity of cyber contest from hostile actors, introducing vulnerabilities into consumer, enterprise, critical infrastructure, military and intelligence networks and data is unacceptable.

Additional lessons learned from the EC experience include:

- **First, the smartphones we use, and the apps they contain, have become integral to nearly every part of our lives today, and every sector of the economy – including within the enterprise and critical infrastructure entities.**

  Because the same device is used across all networks and sectors, any vulnerability introduced into the security of a device for consumers would also be introduced into the same devices used in enterprise, critical infrastructure, military, and intelligence networks. A central and common sense question policymakers need to ask in any proposed new policy – would this policy enhance or undermine trust in hardware, software, products, services across the digital ecosystem?

- **Second, policymakers should thoroughly review government security agency best practices designed to protect the security and privacy of mobile device users and networks before crafting any new policy proposal that would contradict or undermine these proven practices.**

  The DMA experience shows policymakers should not rush into policies that will undermine national and cyber security, pass provisions with inherently contradictory outcomes, or create a policy with no known technical path forward, with the hope that one 'should' be able to do it, particularly policies restructuring core economic industries like the mobile device ecosystem.

- **Third, in the same way that DMA requirements are in tension with GDPR's privacy requirements and considering that the U.S. lacks baseline national privacy requirements similar to the GDPR, U.S. policymakers should make their first priority the adoption and implementation of a comprehensive, effective, and enforceable national privacy framework that protects the privacy of all Americans – across the devices, data and apps they use.**

  Without a comprehensive national privacy framework in place, any steps that undermine the existing official app store privacy protections would make the loss of these existing app store protections even more damaging than the harm that will be caused in the EU, and predictably would accelerate the loss of privacy protections for U.S. citizens.

- **Fourth, given the tension between the DSA's focus on preventing harmful online content, and the DMA's requirement to allow content to be downloaded outside of existing official app store terms and conditions, it is critical that U.S. policymakers understand and avoid steps that could similarly limit the review of apps for harmful, fraudulent, and unlawful content and avoid creating new avenues for the spread of disinformation through apps not subject to app store terms and conditions.**

  After reviewing U.S. proposals with a similar intent as the DMA, a group of U.S. Senators for example warned that U.S. proposals with the same app related goals as the DMA would create unintended consequences and could "supercharge harmful content online" by limiting a company's ability to moderate violative content.

- **Fifth, the DMA was passed by the EU which does not have 'competency' over national security issues.**

  Yet, the DMA has significant national security impacts, and the Member States now have to come in and

try to limit the adverse impact on Member State national security. U.S. policymakers have the advantage of a unitary national security and commercial jurisdiction, and it should make sure national security equities are understood and prioritized upfront, and not adjudicated later, when the security of Americans has been put at risk.

Another base lesson for the U.S. from the passage of the DMA and the implementation issues the EC is struggling with now is that security, privacy, and safety must be the condition precedent to any action – not glossed over to achieve some other policy result.

CONCLUSION

At a time when innovation across hardware, software, networks, and devices is increasingly interdependent, technology governance has become progressively expansive and complex. It is difficult to imagine that any set of laws, rules, or regulations will be able to address the multitude of challenges and often competing objectives. Toward this end, it is useful that the European Commission is holding workshops with experts to better understand these complexities before putting rules into effect. Because without a safe, secure, and trustworthy mobile ecosystem, people will not have the trust necessary to take full advantage of a dynamic, innovative, competitive, equitable, safe, and secure mobile ecosystem that users deserve, and the enterprises demand.

---

[i] Other warnings from official government sources include:

- **DHS's Cybersecurity & Infrastructure Security Agency:** "Avoid potentially harmful apps (PHAs). Reduce the risk of downloading PHAs by limiting your download sources to official app stores, such as your device's manufacturer or operating system app store. Do not download from unknown sources or install untrusted enterprise certificates."
- **FBI's Criminal Justice Information Services Division:** "One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application… Unsigned or untrusted apps are cryptographically prevented from executing on non-jailbroken iOS devices… On either platform, it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy."
- **Commerce Department's National Institute of Standards and Technology:** "Application stores pose an additional threat vector for attackers to distribute malware or other harmful software to end users. This is especially true of third-party application stores not directly supervised by mobile OS vendors… Third-party application stores may be completely legitimate, but may also host applications that commit substantial copyright violations or 'cracked' versions of applications that allow users to install and use paid applications for free."
- **New Zealand's Computer Emergency Response Team:** "Apps that are available from 3rd party sellers may not be legitimate, and could contain malware (like viruses)."