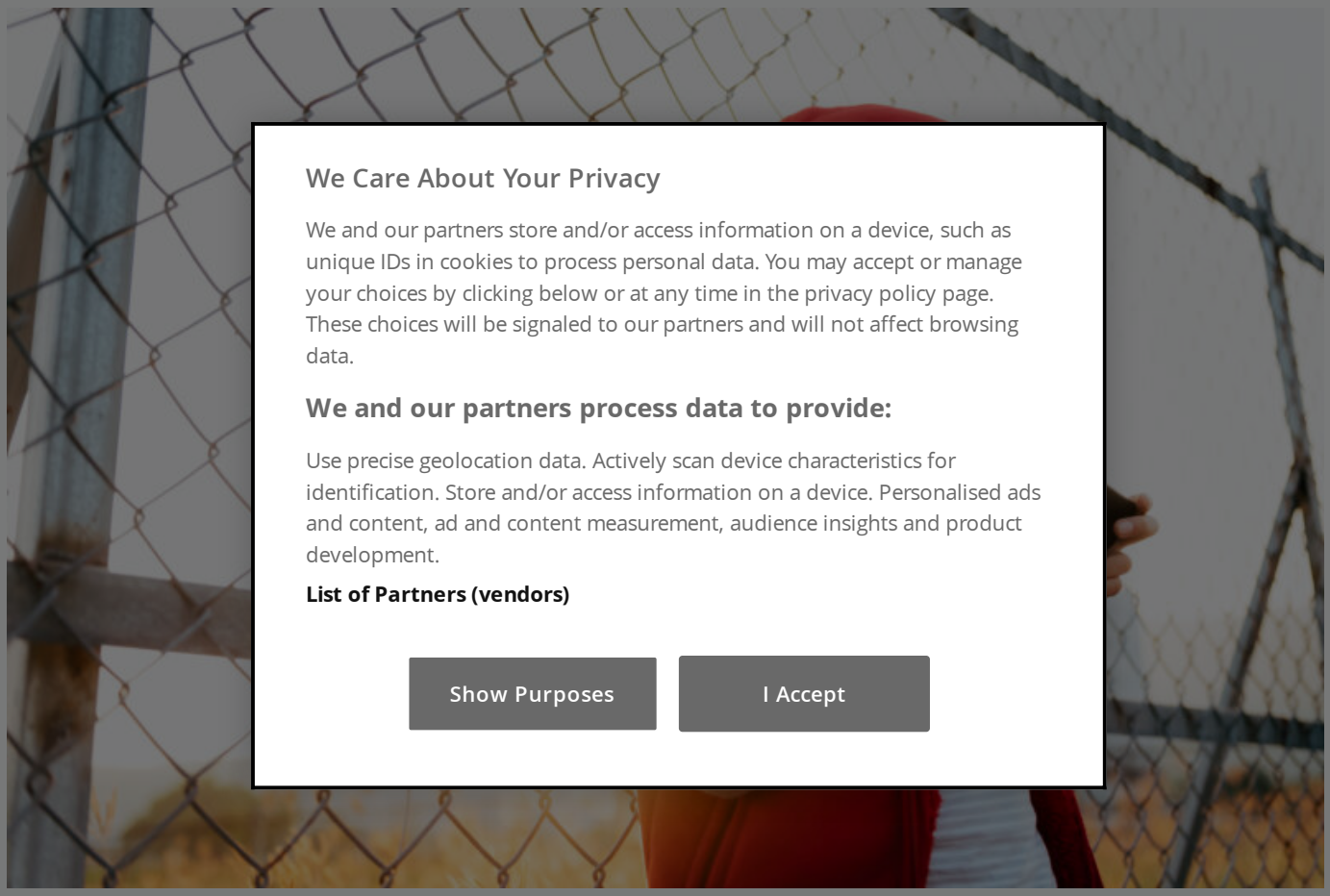
兄, 昆 —

Security s on Chinese

The audit red-flagged Xiaomi and Huawei phones but gave OnePlus a pass.

JIM SALTER - 9/22/2021, 10:30 PM



Clover No. 7 Photography via Getty Images

Enlarge / **Be sure you know what you're getting into before buying and using unfamiliarly branded smartphones—especially international models not originally intended for your country.**

The Lithuanian National Cyber Security Centre (NCSC) recently published a security assessment of three recent-model Chinese-made smartphones—Huawei's P40 5G, Xiaomi's Mi 10T 5G, and OnePlus' 8T 5G. Sufficiently determined US shoppers can find the P40 5G on Amazon and the Mi 10T 5G on Walmart.com—but we will not be providing direct links to those phones, given the results of the NCSC's security audit.

The Xiaomi phone includes software modules specifically designed to leak data to Chinese authorities and to censor media related to topics the Chinese government considers sensitive. The Huawei phone replaces the standard Google Play application store with third-party substitutes the NCSC found to harbor sketchy, potentially malicious repackaging of common applications.

Table 1. Main software characteristics of mobile devices included in the analysis

Name of device	Huawei P40	Xiaomi Mi 10T	OnePlus 8T
Factory-installed OS basis	Android 10	Android 10 (QKQ.200419.0P2)	Android 11
Manufacturer's modification of factory	EMUI 10.1.0	MIUI Global 12.0.10	Oxygen OS B05BA
Latest			d 11
Manufactu latest			n OS KB05AA
Latest ava			4-08
OS			-pref+
security			0-01
Date of mos			1-01[16]
Numbe			

Lithuanian NCSC

Huawei's P40 to 11. Only the OnePlus 8T

The OnePlus 8T 5G e three—was the only one to esc

Xiaomi Mi 10T 5G

Table 13. List of mobile applications using the MiAdBlacklistConfig file

Line No.:	Application name	Application identifier	Device
1	Security	*com.miui.securitycenter*	Xiaomi Mi 10T
2	Mi Browser	*com.mi.globalbrowser*	
3	Downloads	*com.android.providers.downloads.ui*	
4	Music	*com.miui.player*	
5	Themes	*com.android.thememanager*	
6	MIUI Package Installer	*com.miui.global.packageinstaller*	
7	Cleaner	*com.miui.cleanmaster*	

Lithuanian NCSC

The NCSC found that seven default system apps on the Xiaomi phone can monitor media content for blocking from the user, using a regularly downloaded JSON file.

Xiaomi's Mi 10T 5G ships with a nonstandard browser called "Mi Browser." The NCSC found two components in Mi Browser which it didn't like—Google Analytics, and a less familiar module called Sensor Data.

The Google Analytics module in Mi Browser can read from the device's browsing and search history and can then send that data to Xiaomi servers for unspecified analysis and use. The Google Analytics module is activated automatically by default during the phone's first activation or after any factory reset.

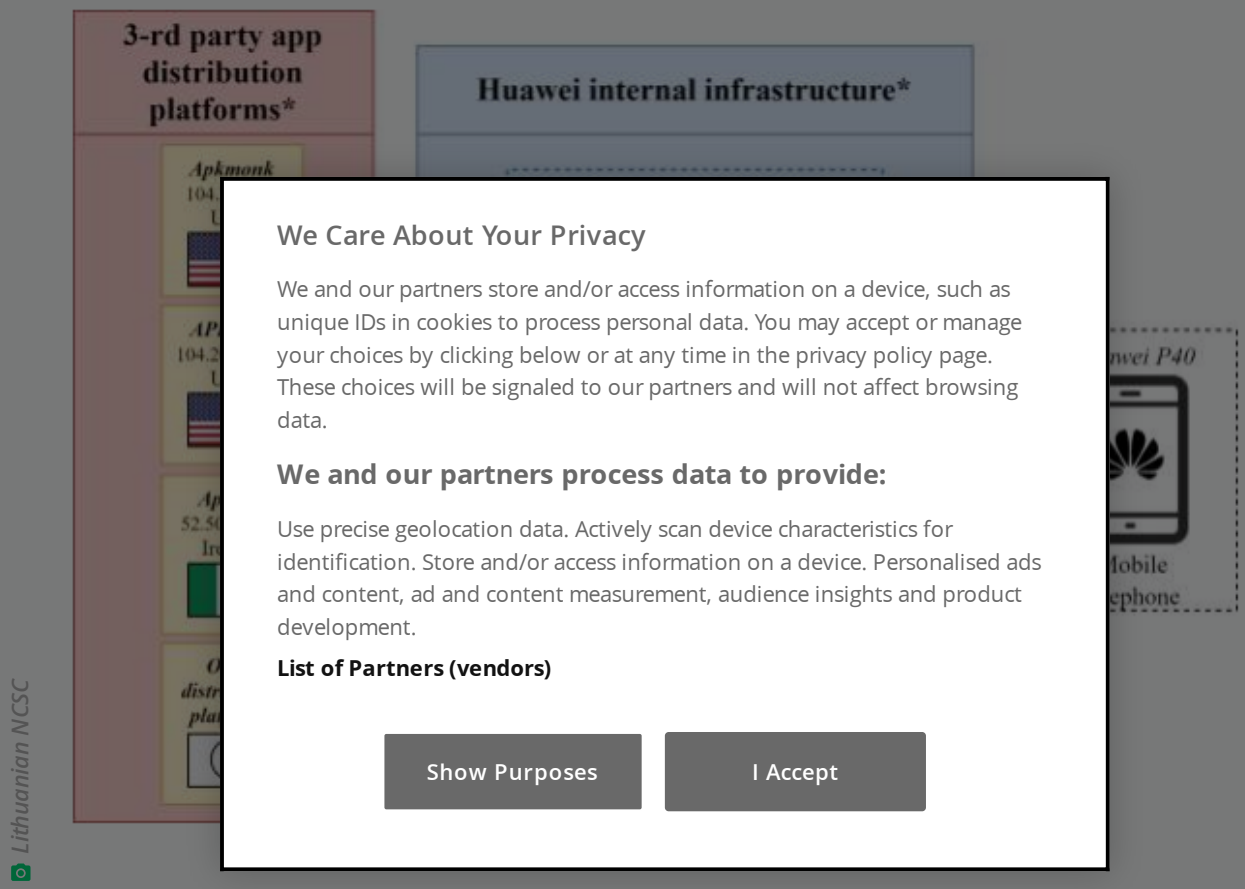
The NCSC found tha l to application activity, including ti are encrypted and sent to Xiaomi d by the EU's GDPR and has beer

The NCSC also foun vers in Singapore via encrypted SMS phone number is sent whether the user ties it to a new cloud account or not, and the encrypted SMS is not visible to the user.

Several of the Xiaomi system applications on the Mi 10T 5G regularly download a file called MiAdBlackListConfig from servers in Singapore. In this file, the NCSC found 449 records identifying religious, political, and social groups. Software classes in these Xiaomi applications use MiAdBlackListConfig to analyze multimedia which might be displayed on the device and block that content if "undesirable" keywords are associated with it.

Although the NCSC discovered that the actual content filtering via MiAdBlackListConfig is disabled on phones registered in the European Union, the phones still regularly download the blocklist itself—and, the agency says, can be remotely reactivated at any time.

Huawei P40 5G



The NCSC found that users who search for applications in Huawei's AppGallery are often redirected to potentially untrustworthy third-party repositories.

Although the NCSC did not find the same class of spyware and content-filtering modules in Huawei's P40 5G as it had in the Mi 10T 5G, it still wasn't happy with the phone's software infrastructure—and for good reason.

The P40 5G's most obvious problems stem from its replacement of Google's Play Store with Huawei's own AppGallery store, which it bills as "a safer place to get all your favorite apps." The NCSC found that, if a user searches AppGallery for a particular application, they will be silently redirected to third-party app stores if no match is found in AppGallery itself.

Third-party distribution platforms the NCSC found linked to AppGallery include but are not limited to Apkmonk, APKPure, and Aptoide. The NCSC used VirusTotal to scan several apps installed via AppGallery and its linked third-party platforms, and it discovered potential malware on three: All in One social media, C -One, Live Free Chat Pro App."

We're not certain h nce the agency did not reverse eng se positives on less well-known ap king from AppGallery to third ise.

Although Apkmonk ores," they're less thoroughly cur th its own main repository—which t Aptoide also allows easy self-ho —whether they're a user want r a developer hosting their own c

The ease of reposit d apps on its user repositories— rity risk, particularly when those users might not realize they've left the safety of the mainstream in the first place.

Even users not looking for pirated software may inadvertently stumble on malware-added repackaging or copycat versions of legitimate applications, with apparent "legitimacy" added by re-signing the modified or copycat application with the uploader's own key.

Conclusions

Based on the NCSC's findings, there doesn't seem to be any issue with the OnePlus phone—which comes as little surprise, as it's the only brand of the three which hasn't come under repeated, negative scrutiny from non-Chinese administrations.

Particularly adventurous and/or Google-hating consumers might reasonably be interested in Huawei's P40, which seems afflicted more with a lack of malware-preventing guardrails than with actual directly imposed censorship and/or spyware.

Finally, we'd strongly advise avoiding the Xiaomi Mi 10T—its deactivated but regularly updated blocklist functionality strikes us as a warning of direct authoritarian oversight which should not be lightly ignored.

JIM SALTER

Jim is an author, podcaster, mercenary sysadmin, coder, and father of three—not necessarily in that order.

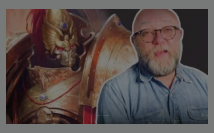
EM

CHANNEL ars

Unsolved Mysteries Of Quantum Leap With Donald P. Bellisario

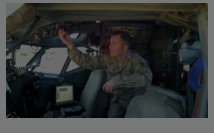
Today "Quantum Leap" series creator Donald P. Bellisario joins Ars Technica to answer once and for all the lingering questions we have about his enduringly popular show. Was Dr. Sam Beckett really leaping between all those time periods and people or did he

Unsolved Mysteries Of Quantum Leap With Donald P. Bellisario



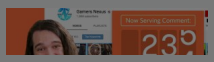
Unsolved Mysteries Of Warhammer 40K With Author Dan Abnett

SITREP: F-16 replacement search a signal of F-35 fail?



Sitrep: Boeing 707

simply imagine it all? What do people in the waiting room do while Sam is in their bodies? What happens to Sam's loyal ally AI? 30 years following the series finale, answers to these mysteries and more await.



Steve Burke of

More videos

← PREVIOUS S

XT STORY →

Related Stor

Today on Ar

Join the Ars Orbital Transmission mailing list to get weekly updates delivered to your inbox.

SIGN ME UP →

CONDÉ NAST