HITB SECCONF SIN-2021

Stay Off My Private Data:

A Framework to Examine Mobile App Privacy Claims

Bai Guangdong@UQ | Zhang Qing@ByteDance | Wang Zeyu@ByteDance

TRACK 2

About Us

Bai Guangdong

Senior Lecturer from

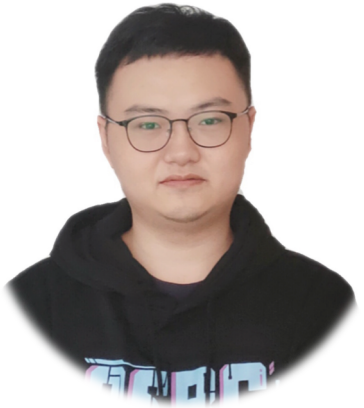
The University of Queens & Australia

Research on mobile security & protocol analysis

Zhang Qing

Senior security researcher from ByteDance

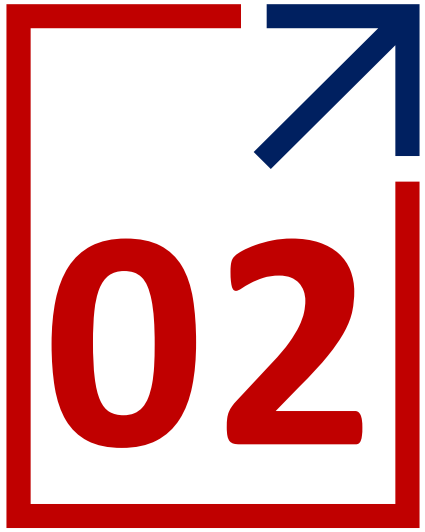
Research on Mobile security & payment security



Wang Zeyu

Senior security researcher from ByteDance

Research on Android application security & privacy protection



Background

This video clip is from the film Jexi(https://en.wikipedia.org/wiki/Jexi).
Jexi is a 2019 romantic comedy film written and directed by Jon Lucas and Scott Moore.

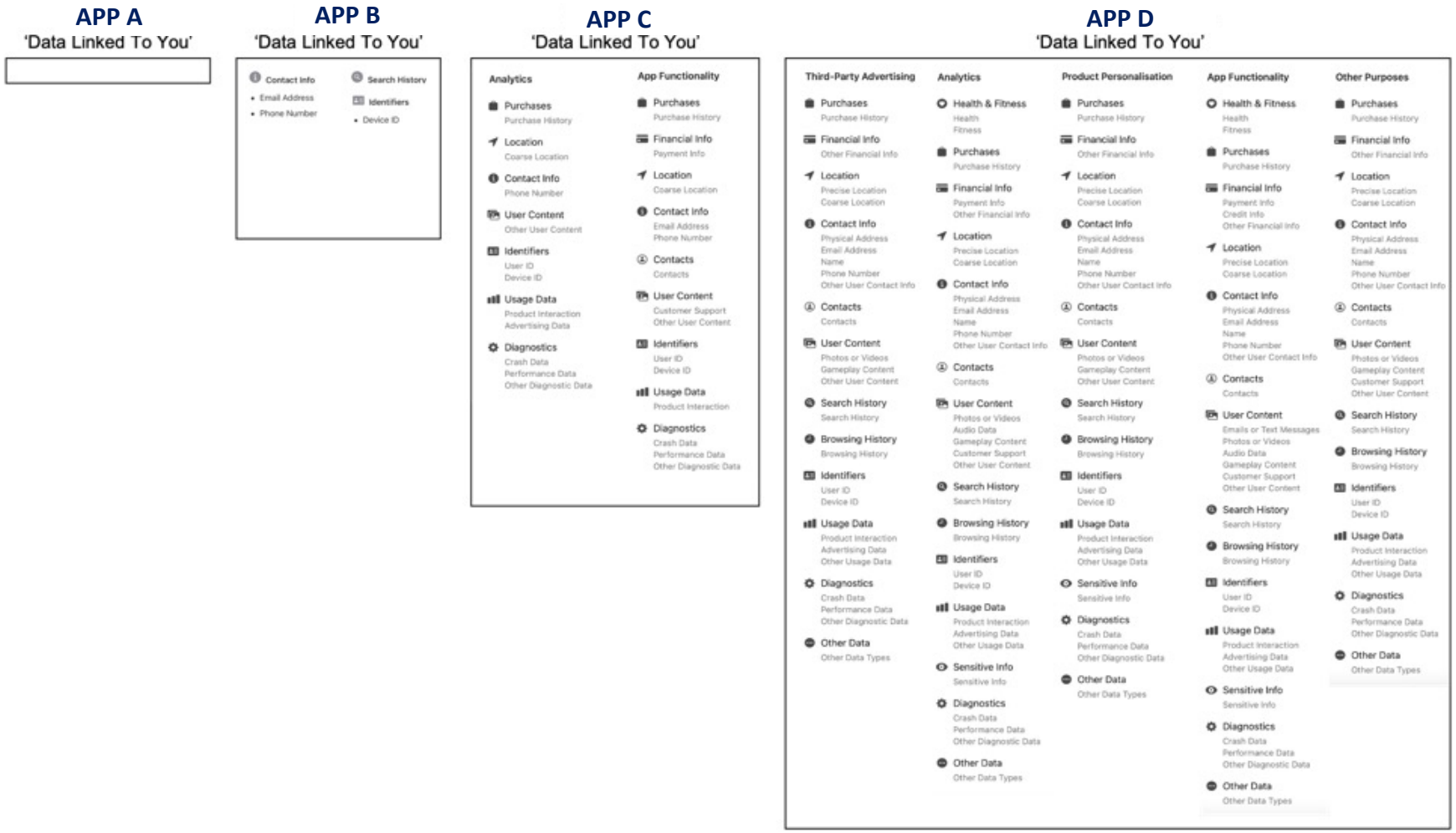
Applications are collecting your data

A variety of data types

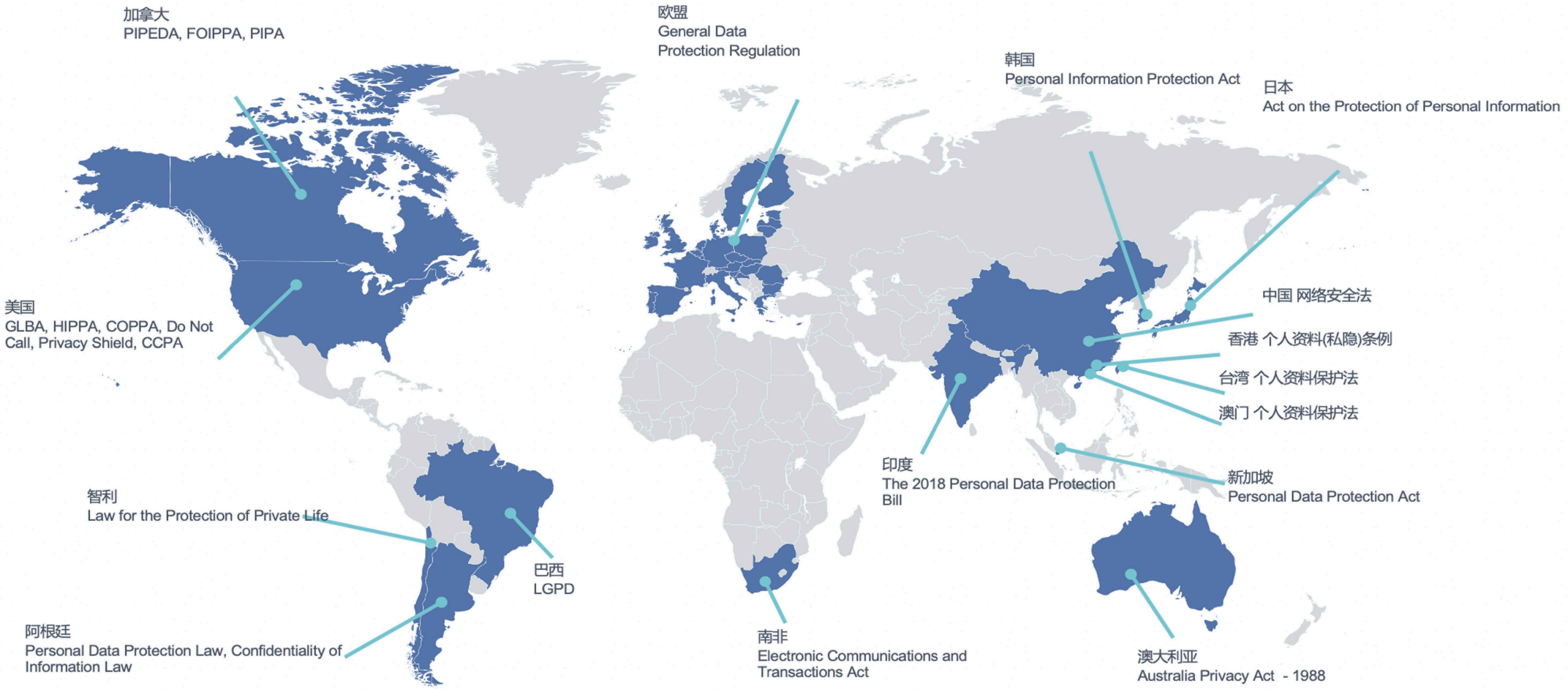
- Location
- Device ID
- SIM info
- Browsing history

A variety of purposes

- Analytics
- App functionality
- Product personalization
- Third-party advertising



Data protection regulations are global



European General Data Protection Regulation (GDPR)

- GDPR legislation came into force on May 2018 in European Union (EU) countries
- A major update to the EU Data Protection Directive (95/46/EC) (DPD-95) introduced in 1995
- Covers six aspects

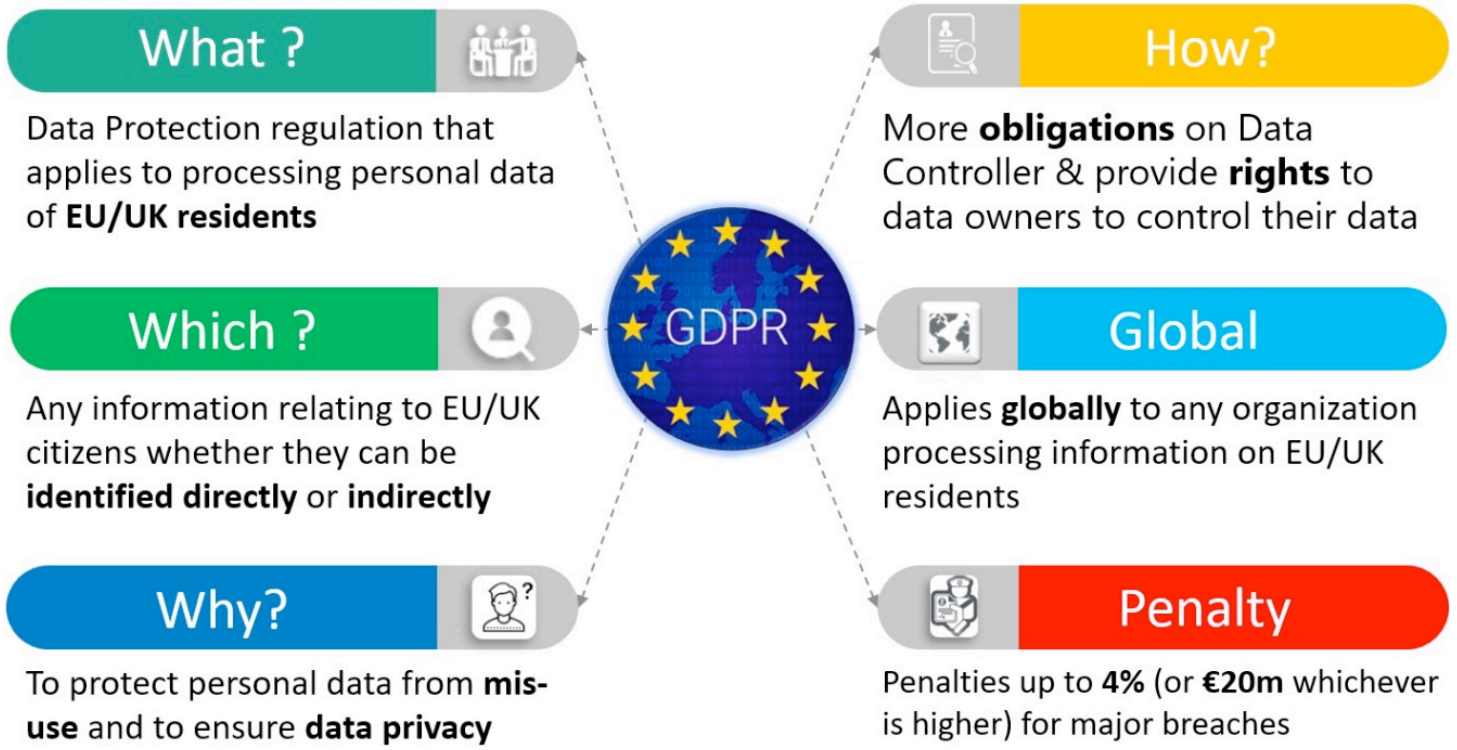


Figure source: Truong, N., Sun, K., Wang, S., Guitton, F. & Guo, Y., 2020. Privacy Preservation in Federated Learning: Insights from the GDPR Perspective. arXiv preprint arXiv:2011.05411.

GDPR Principles

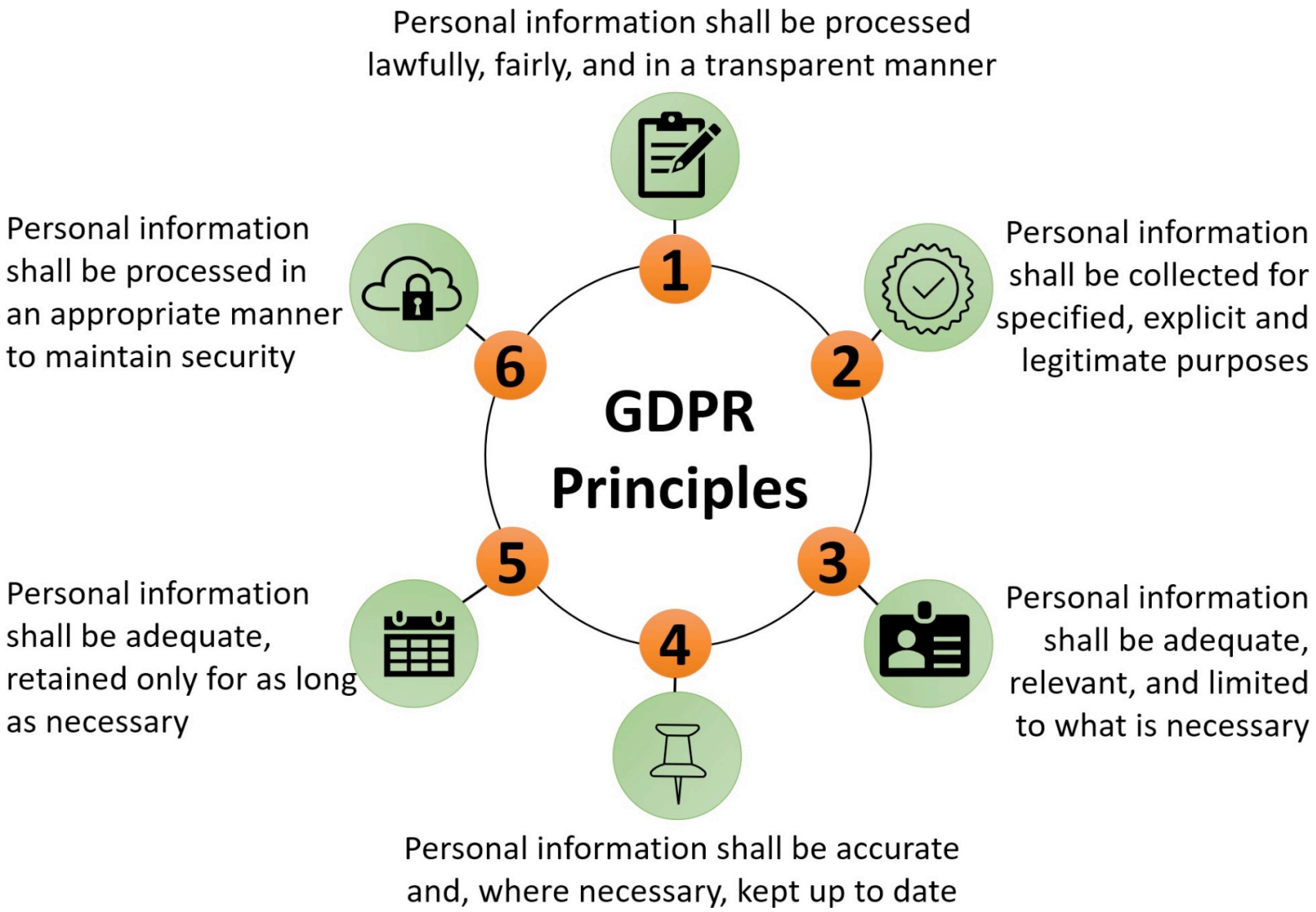


Figure source: Truong, N., Sun, K., Wang, S., Guitton, F. & Guo, Y., 2020. Privacy Preservation in Federated Learning: Insights from the GDPR Perspective. arXiv preprint arXiv:2011.05411.

US California Consumer Privacy Act (CCPA) & US Children's Online Privacy Protection Rule (COPPA)

Similar to GDPR, with minor differences in scope, key definitions, legal basis, rights & enforcement.

Scope

- GDPR: “an identified or identifiable natural person”
- CCPA: “a natural person who is a California resident.”

Region

- GDPR: both “entities or organizations” “established” or “not established” “in the EU”
- CCPA: “doing business in California.”

Google Play's Requirements for Privacy Policies

4.8

- You agree that if You make Your Products available through Google Play **You will protect the privacy & legal rights of users.** If the users provide You with, or Your Product accesses or uses, usernames, passwords, or other login information or personal information, **You agree to make the users aware that the information will be available to Your Product, & You agree to provide legally adequate privacy notice & protection for those users.** Further, Your Product may only use that information for the limited purposes for which the user has given You permission to do so**. If Your Product stores personal or sensitive information provided by users, You agree to do so securely & only for as long as it is needed.** However, if the user has opted into a separate agreement with You that allows You or Your Product to store or use personal or sensitive information directly related to Your Product (not including other products or applications), then the terms of that separate agreement will govern Your use of such information. If the user provides Your Product with Google Account information, **Your Product may only use that information to access the user's Google Account when, & for the limited purposes for which, the user has given You permission to do so.**

Data Collection & Storage

- What data is collected?
- What the data is used for?
- Who is the data shared with?
- How is the data is protected?

https://play.google.com/intl/ALL_us/about/developer-distribution-agreement.html

Google Play's Policy on User Data

User Data

You must **be transparent** in how you handle user data (e.g., information collected from or about a user, including device information). That means **disclosing your app's access, collection, use, & sharing of the data, & limiting the use of the data to the purposes disclosed.** In addition, **if your app h&les personal or sensitive user data, please also refer to the additional requirements in the "Personal & Sensitive Information" section** below. These Google Play requirements are in addition to any requirements prescribed by applicable privacy & data protection laws.

https://support.google.com/googleplay/&roid-developer/answer/10144311?visit_id=637523214929913988-659406915&rd=1#!?zippy_activeEl=personal-sensitive#personal-sensitive

Personal & Sensitive Information

Personal & sensitive user data includes, but isn't limited to, personally identifiable information, financial & payment information, authentication information, phonebook, contacts, device location, SMS & call related data, microphone, camera, & other sensitive device or usage data. If your app handles sensitive user data, then you must:

- Limit your access, collection, use, & sharing of personal or sensitive data acquired through the app to purposes directly related to providing & improving the features of the app (e.g., user anticipated functionality that is documented & promoted in the app's description in the Play Store). Apps that extend usage of this data for serving advertising must be in compliance with our Ads Policy.
- Post a privacy policy in both the designated field in the Play Console & within the app itself. The privacy policy must, together with any in-app disclosures, comprehensively disclose how your app accesses, collects, uses, & shares user data. Your privacy policy must disclose the types of personal & sensitive data your app accesses, collects, uses, & shares & the types of parties with which any personal or sensitive user data is shared.
- Handle all personal or sensitive user data securely, including transmitting it using modern cryptography (for example, over HTTPS).
- Use a runtime permissions request whenever available, prior to accessing data gated by Android permissions.
- Not sell personal or sensitive user data.

Privacy policy common themes

Our policy on children's data

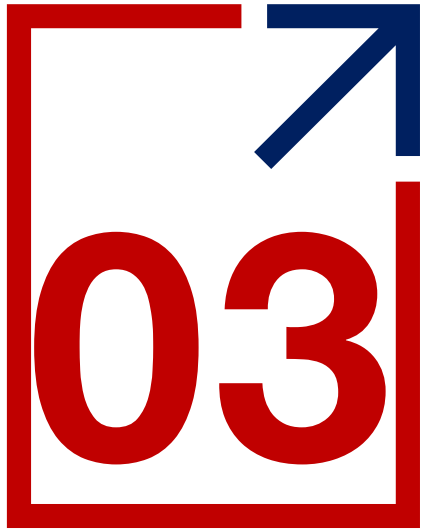
What we do with the data we collect

Choices you have about your data

How & when we share your data

How long we retain your data

How to download your data



The Framework

Motivation

When conducting an application privacy compliance audit, how do we ensure that testing covers the majority, if not all privacy compliance issues?

Challenges

From regulations to best practice:

- Regulations are abstract, theoretical, & complex.
- Regulators mainly focus on enacting the laws & demand reliable regulation/auditing technologies.

From passive to active:

- Privacy challenges may often be remediated in a passive way of patching when vulnerabilities are discovered, like a whack-a-mole game.
- May lack a systematical approach to actively enforce the protection proactively.

From research to application:

- Many privacy incidents are exposed by researchers, where manual efforts are needed
- We summarize the complex privacy security audit methodology in a systematic framework based on our experience with a large number of app privacy security audits.

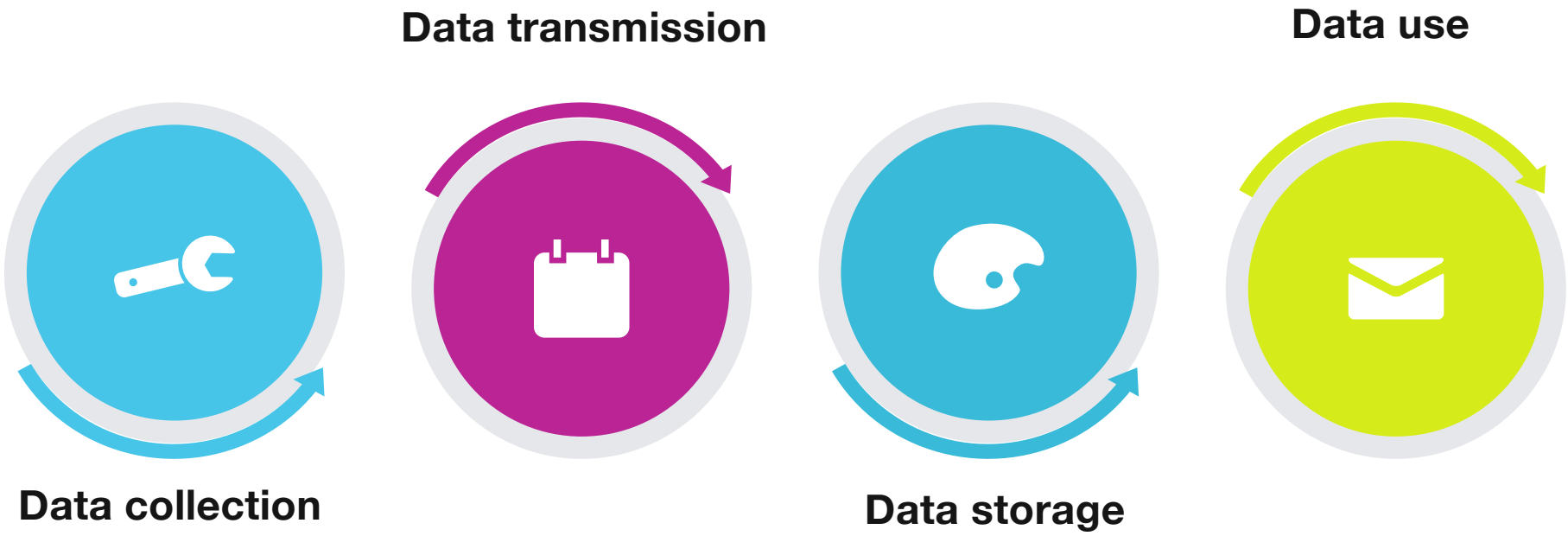
Global view & guidelines

- Global view: take the entire data lifecycle into consideration.
- Guideline: break it down into an enforceable check list.

Our framework

- **Logic level:** allows decision makers to have a big picture view of potential scenarios where privacy issues may occur.
- **Enforcement level:** guides auditors/analysts to make inspections in an efficient & comprehensive way.

Logic level: data lifecycle



Including whether apps **provide users choice & control** over how/when their data is acquired, accessed, retained, stored, erased, & localized.

Logic level break-down

Type	Item	Description	Test method
Illegal collection of user data	Collection or use of data is beyond scope of user authorization.	Actual collection of users' personal data by app goes beyond types of data listed in the privacy statement.	Manual work
	Collection of personal data without user consent or authorization.	Collection personal data without the user's consent, or after the user has expressly refused to do so.	Automation tools & manual work
	Purpose & scope of collection & use of personal information are not stated.	Rules for personal data collection & use of app do not list the purpose, method, & scope of personal data collection & use or relevant permissions individually.	Manual work
	Compulsory granting permissions related to user data, or requesting permission related to user info without using it.	Continued request for permissions, or requesting permissions but not using related functions.	Manual work
Illegal use of user data	Force users to use directed push.	No option to turn off directional push is provided. The collected user privacy information which is not marked in a significant way & without the user's consent is used for targeted push or targeted advertising marketing.	Manual work
	Providing personal data to others without users' consent.	Providing users' personal data to others or third party SDKs without users' consent.	Automation tools & manual work
Illegal transfer of user data	Transmission of sensitive data in clear text.	Using http or insecure https to transfer private user data.	Automation tools &manual work
	Storage & requesting of resources across borders.	Storing & requesting resources across borders.	Automation tool & manual work
Illegal storage of user data	Storage of sensitive data in SD card.	Storing sensitive data in SDcard leading to the data to be obtained by other third-party application.	Automation tool & manual work
	Deletion of user data without permission.	Deleting ser data in the SDcard without permission.	Manual work

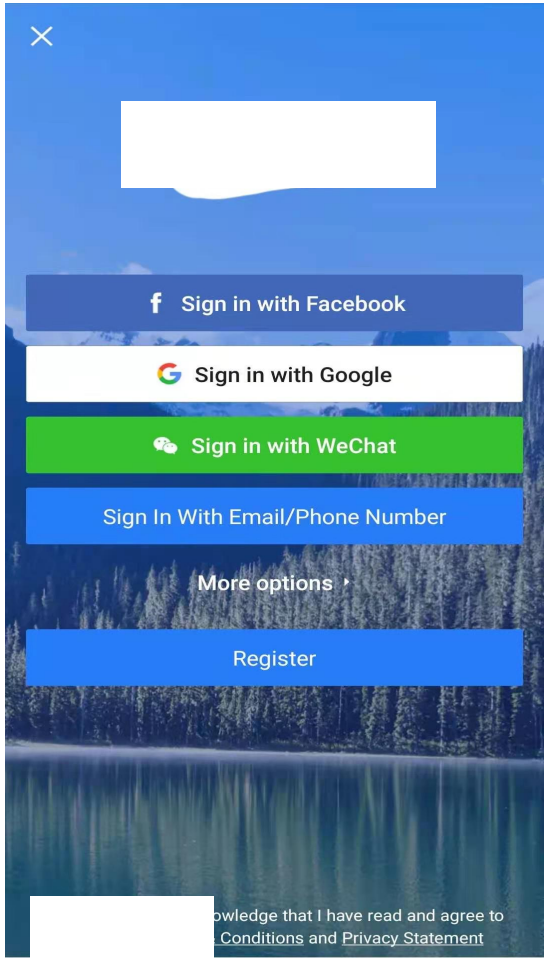
Enforcement level

Type	Item	Description	Test method
Network request	Uploading user data	Statistics & log service uploads user data such as messages, credit card data etc. to third-party servers. Requesting third party links with cookies.	Manual work
		Video data such as drafts & screenshots are automatically uploaded to the server without authorization.	
	HTTP, WS plaintext transmission or unencrypted financial data transferred to server		
	Overseas data communication		
	Certificate validation concerns		Manual work
	Elevation of Privilege to get users' sensitive data	Using add, get, set, & change APIs to obtain users' sensitive data	Manual work
Privacy policy	Collect personal information without user consent or authorization.	Such as MAC address, SSID, BSSID, Android_ID, openUID, packagelist, clipboard, serial number, etc.	Automation tools
	Other items in the logical classification about supervision requirements.		Manual work
Application permissions	Using permissions before user agreement		Manual work
	Requesting the permission when not using the related functions, such as location, SMS, etc.		
	If user does not agree to enable other permissions beside the minimum necessary permissions for app, & the App won't work.		
	Keeping requesting permissions after rejection		
Hard code	oversea domains & IP addresses, userinfo, test codes hard code in the application		Automation tools & manual work
App log	App log prints users' private information		Manual work
Excessive data request	Frequently reading call logs, locations, clipboard		Automation tools

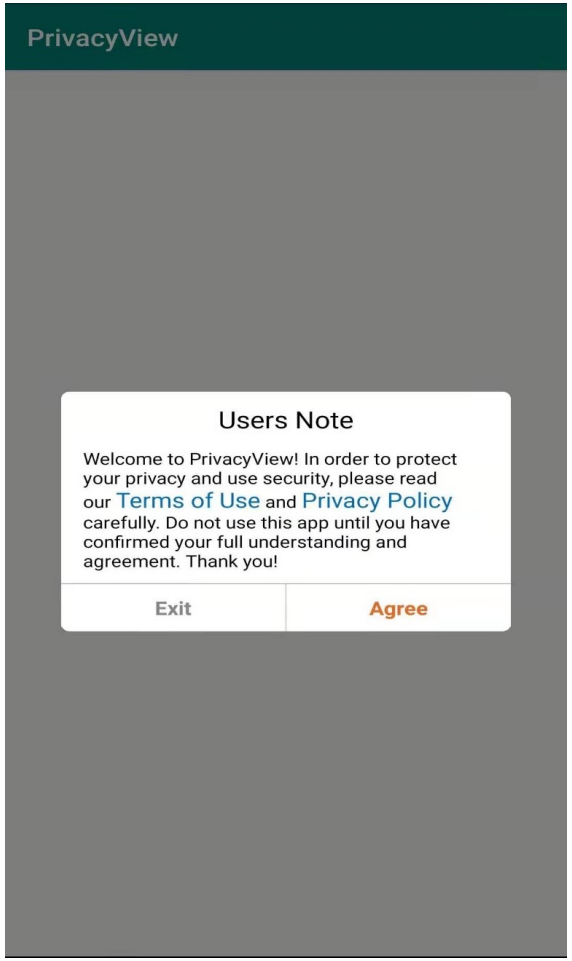
Enforcement level: Example

Network request	Uploading user data	Statistics & log service to upload user data such as messages, credit card data to third-party servers. Requesting third party link with cookie.
		Video data such as drafts & screenshots automatically uploaded server without authorization.
	HTTP, WS plaintext transmission or unencrypted financial data transferred to server	
	Elevation of privilege	Using add, get, set, & change APIs to obtain users' sensitive data

Privacy principles in different countries



US & other countries



China

Automated tools used in the framework

Name	Function
Domain test tool	Obtain all IP addresses & domains from application to check if they belong to trustworthy entities.
Privacy pop-up window test tool	Test if the application obtains user's privacy information before user agrees to privacy policy using hook.
Application scan tool	Check all the APIs related to privacy & validate if the application has certificate validation concerns
Traffic detection tool	Obtain all network traffic of the application when running.

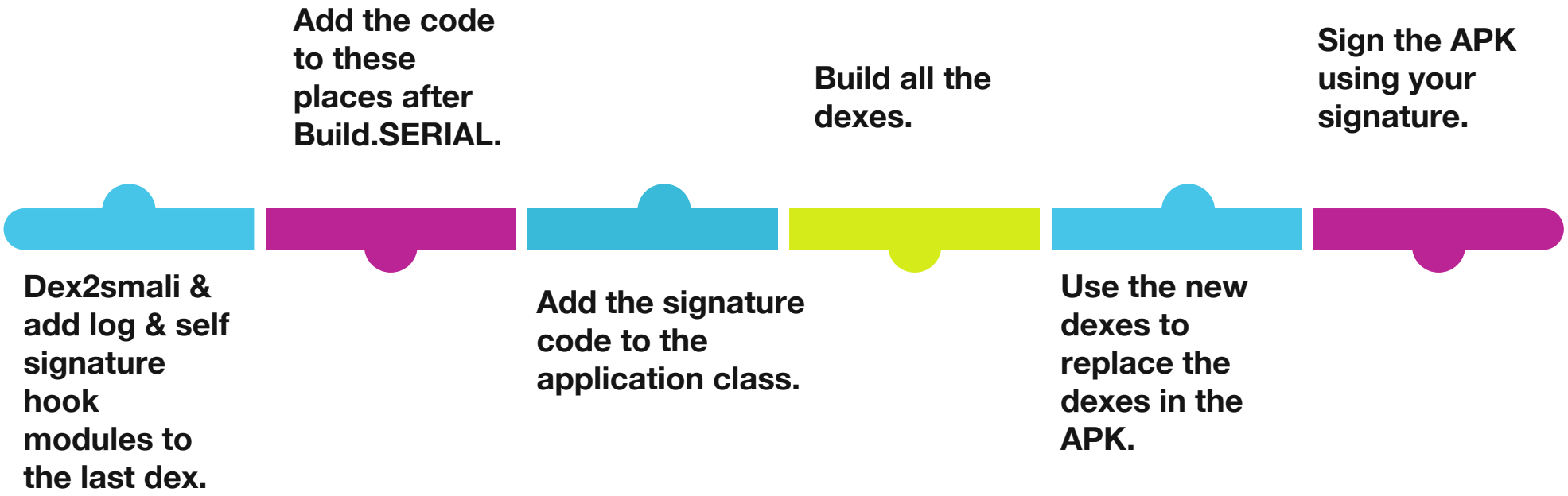
Common private data permissions

Dangerous Permission	Normal Permission	Function
serial_number	**serial_number (No any permission needed)**	Build.getSerial() ro.serialno ro.boot.serialno Build.SERIAL
Imei/Meid	**Mac address/Bssid/Ssid**	Mac:/sys/class/net/wlan0/address Mac:getNetworkInterfaces() Router Mac:/proc/pid/net/arp DEVICE_ID≈IMEI≈MEID≈ESN
Imsi/Iccid/Phone number	**Android_id/Openudid (No any permission needed)**	Android_id≈Openudid
Location	**Package list (No any permission needed)**	List:Pm list
SMS/Call Log	**ClipBoard (No any permission needed)**	getPrimaryClip()

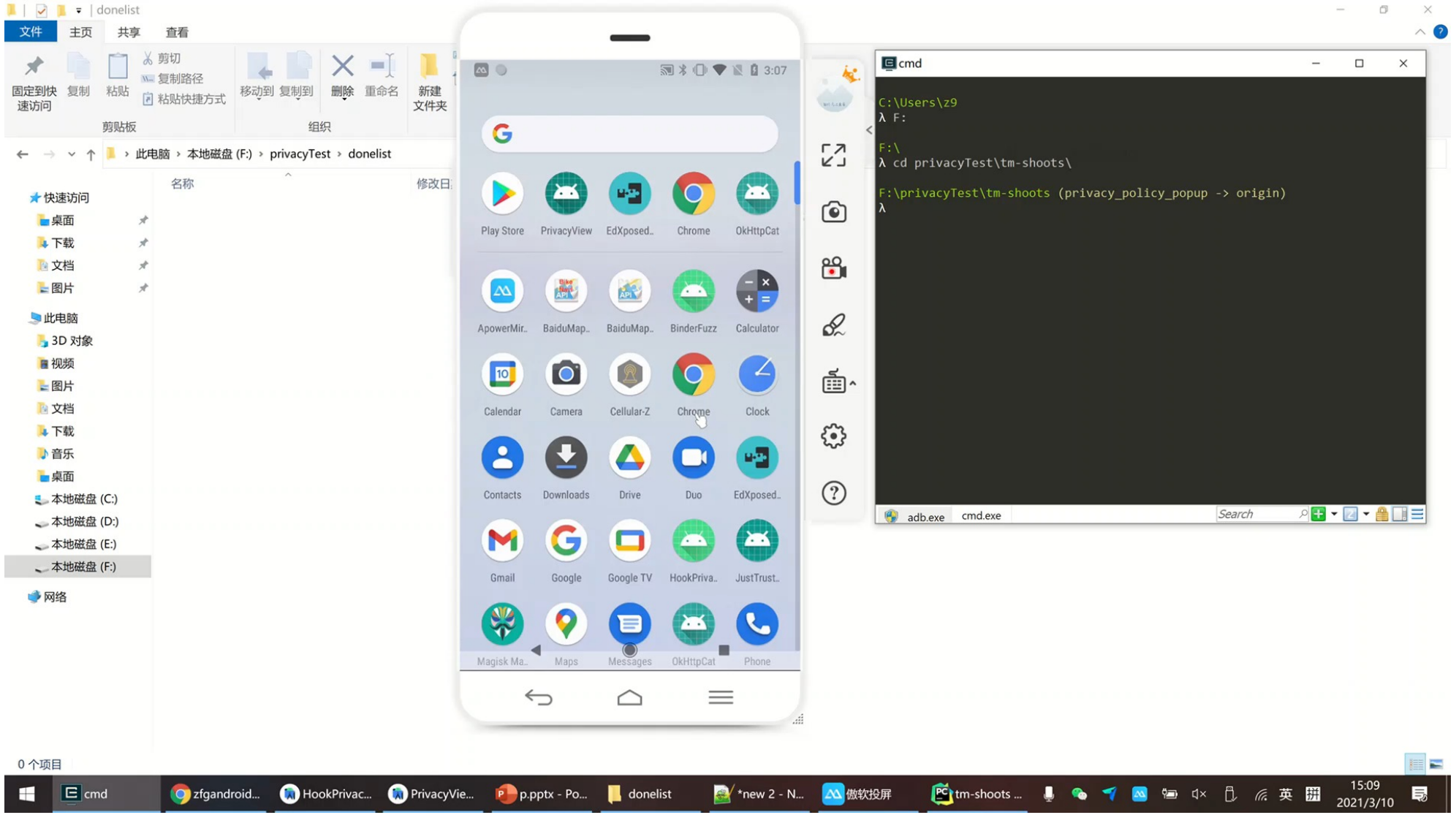
How can I tell if a static variable is being called?

Static variable can **not** be hooked by Frida or Xposed.

New instrumentation technology：



Automated tools in the framework

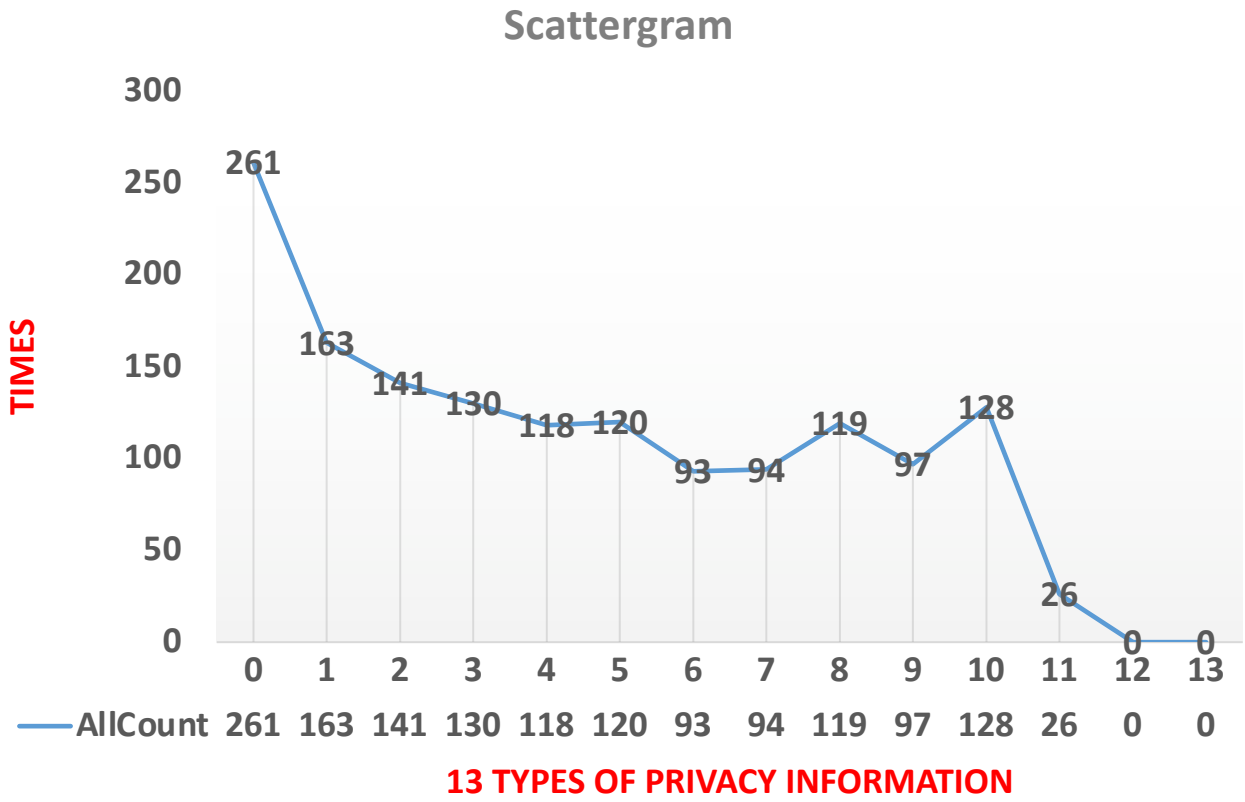


Statistical results

Description	API
Task	1.getRunningAppProcesses 2.getRunningTasks 3.getRunningServices 4.getRecentTasks
Wi-fi	1.getSSID 2.toString 3.getScanResults 4.getExtraInfo 5. getBSSID 6./net/arp 7. getHardwareAddress 8./sys/class/net/wlan0/address
Applist	1.getInstalledPackages 2.queryIntentActivities 3.getInstalledApplications 4.list package
ANDROID_ID	1.Settings.System.getString(context.getContentResolver(), Settings.System.&ROID_ID)
SystemProperty	getprop
serial_no	1.Build.SERIAL 2.ro.serialno 3.ro.boot.serialno 4. Build.getSerial
ClipBoard	1.setPrimaryClip 2.getPrimaryClip
Sensor	1.registerListener 2.requestTriggerSensor 3.registerDynamicSensorCallback
Location	1.getLatitude 2.getLongitude 3.getCellLocation 4.getAllCellInfo
IMEI	1.getImei 2.getDeviceId 3.getMeid
SimcardInfo	1. getSimSerialNumber iccid 2. getSubscriberId 3. getLine1Number
Contact&SMS	1.content://com.&roid.contacts/contacts 2.content://com.&roid.contacts/raw_contacts 3.content://com.&roid.contacts/data 4. content://call_log/calls 5.content://mms 6.content://mms-sms 7.content://sms
Calendar	1.content://com.&roid.calendar/events 2.content://com.&roid.calendar/reminders

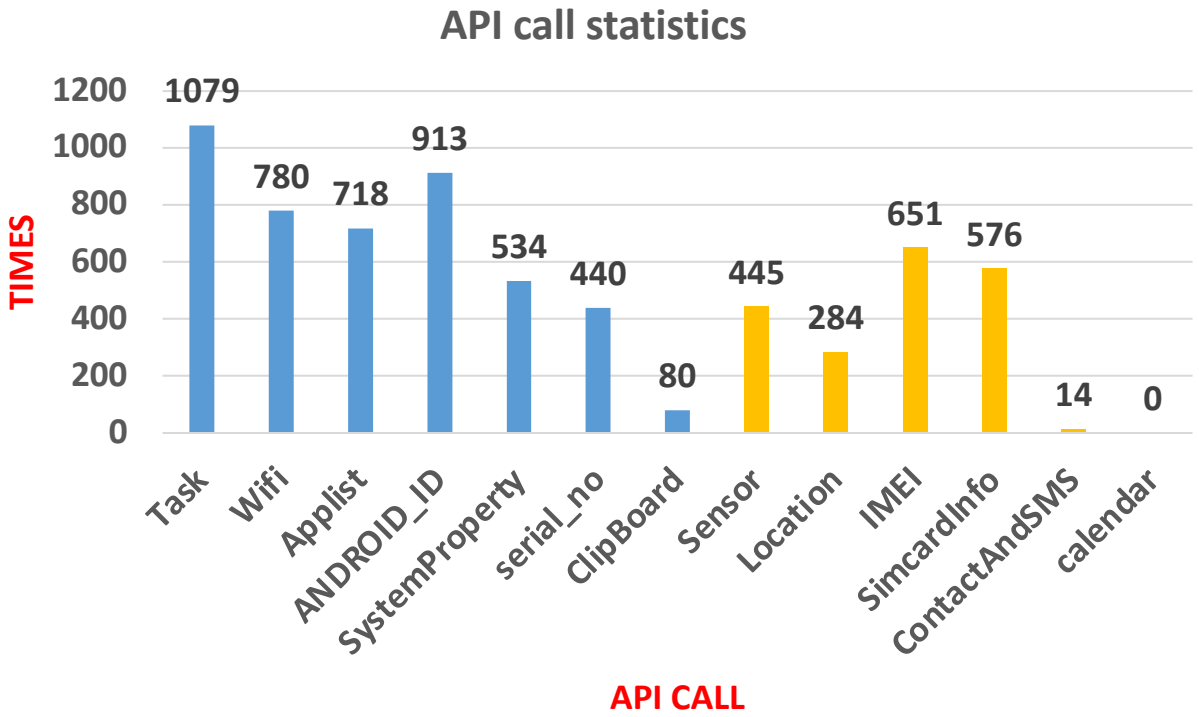
Statistical data

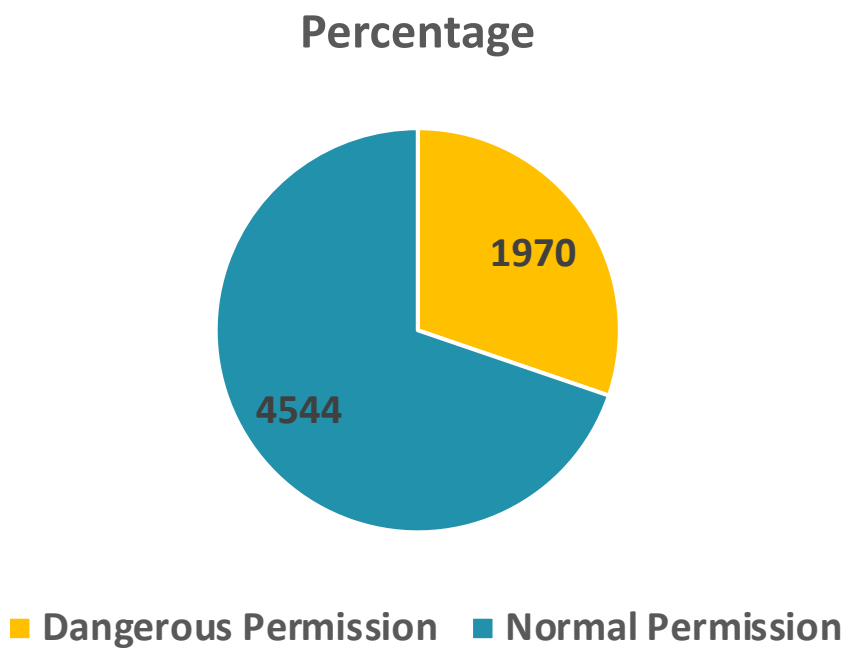
Name	Times
Target App	1,490
Effected App	1,229
Effected App(Except task and SystemProperty)	1041
Using unnormal API App	579



Top 1,490 Apps from Google Play Store & other app stores.

Statistical data





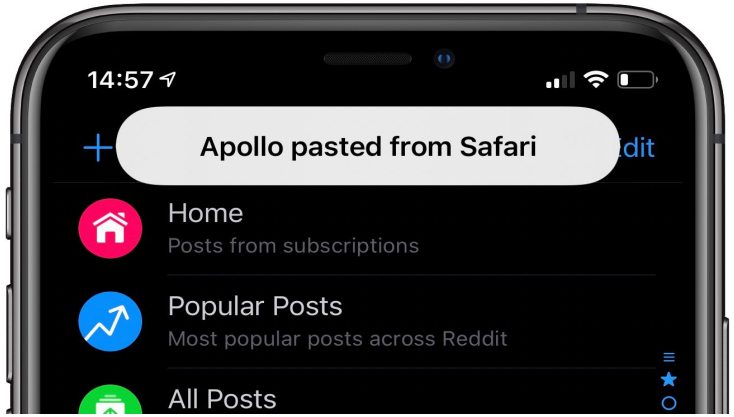
Summary & Recommendations

Advantages

- Cover as many app privacy audit scenarios as possible.
- Provide the analyst a big picture on items audited.

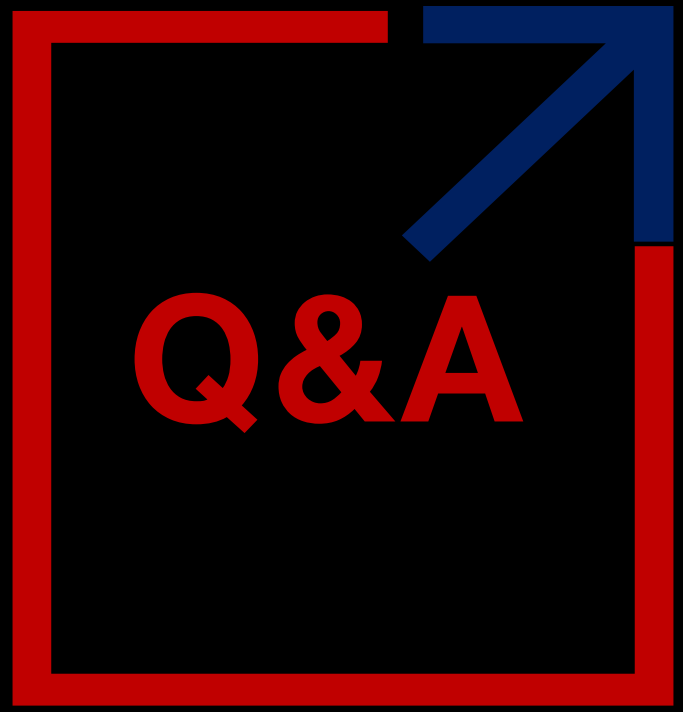
Recommendations to mobile device users

- Update Android OS to Android 10 or Android 11.
- Update iOS device to iOS14.
- Latest versions of both Android & iOS enforce strict regulations on apps.
- Review & update native privacy settings on iOS & Android
- Review & update app privacy settings.



✓	**Background location access** Android 11 changes how users can grant the background location permission to apps	Apps that target Android 11 or higher and need access to background location	Request foreground (coarse or fine) and background location permissions incrementally in separate calls to the permission request method. When necessary, explain the benefits that users receive for granting that permission Learn more about background location access in Android 11
✓	**Package visibility** Android 11 changes how apps query and interact with other installed apps on the same device	Apps that target Android 11 or higher and interact with other installed apps on a device	Add the `<queries>` element to your app's manifest Learn more about package visibility
✓	**Foreground services** Android 11 changes how foreground services can access location, camera, and microphone data	Apps that run on Android 11 or higher and access location, the camera, or the microphone in a foreground service	Declare the `camera` and `microphone` foreground service types for the foreground services that require access to the camera and microphone, respectively. Be aware, however, that foreground services that start while the app is in the background usually cannot access location, camera, or microphone. Learn more about the changes to foreground services

HITB SECCONF SIN-2021



Thank You!