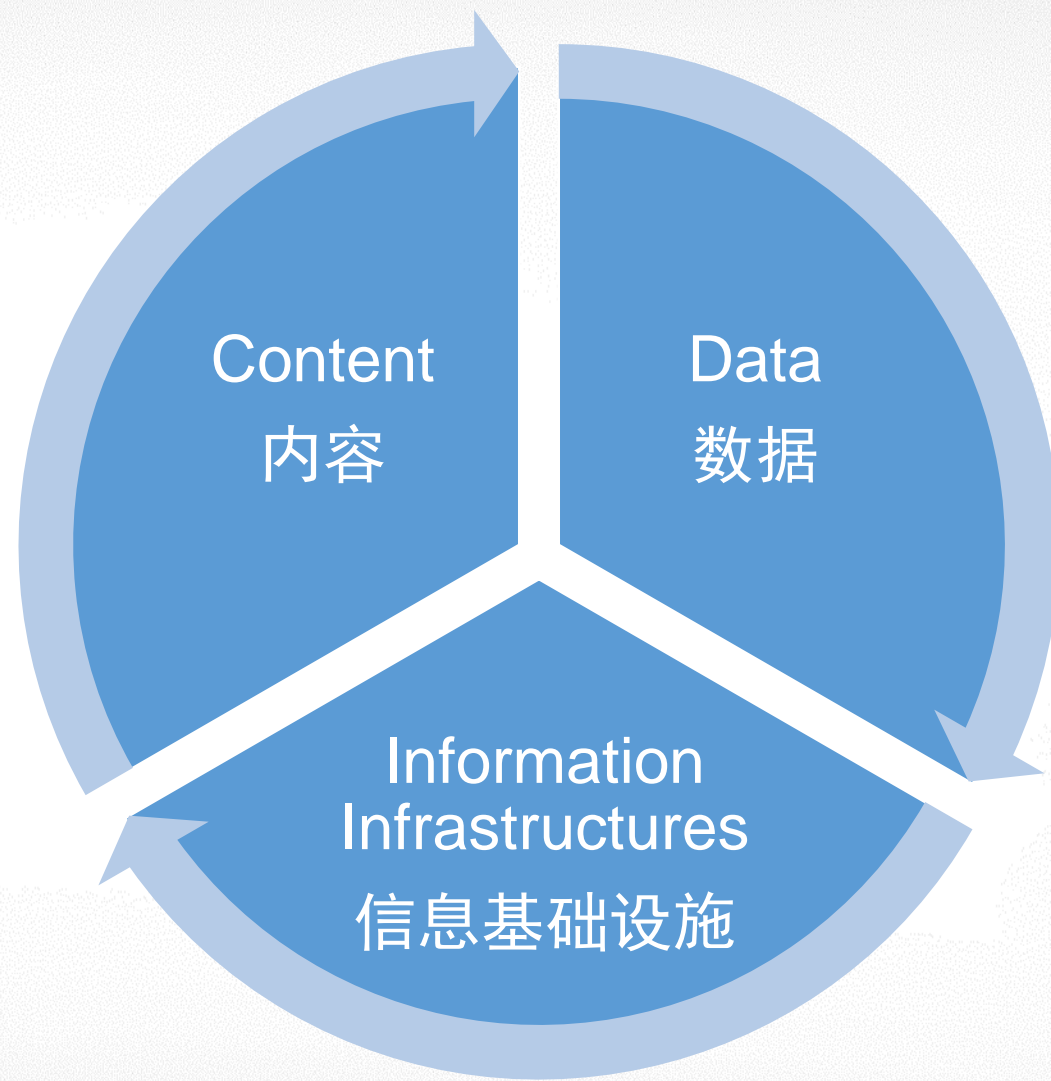


Introduction to Regulations and Enforcement on Data Security and Privacy in China

Dr. HONG Yanqing

2023-05-17



Content
内容

Data
数据

Information
Infrastructures
信息基础设施

Legal Framework on Information Infrastructures

《计算机信息系统安全
保护条例》 (1994)

Regulations of the
People's Republic of
China on Protecting the
Safety of Computer
Information Systems

《计算机信息网络国际
联网安全保护管理办法》
(1997)

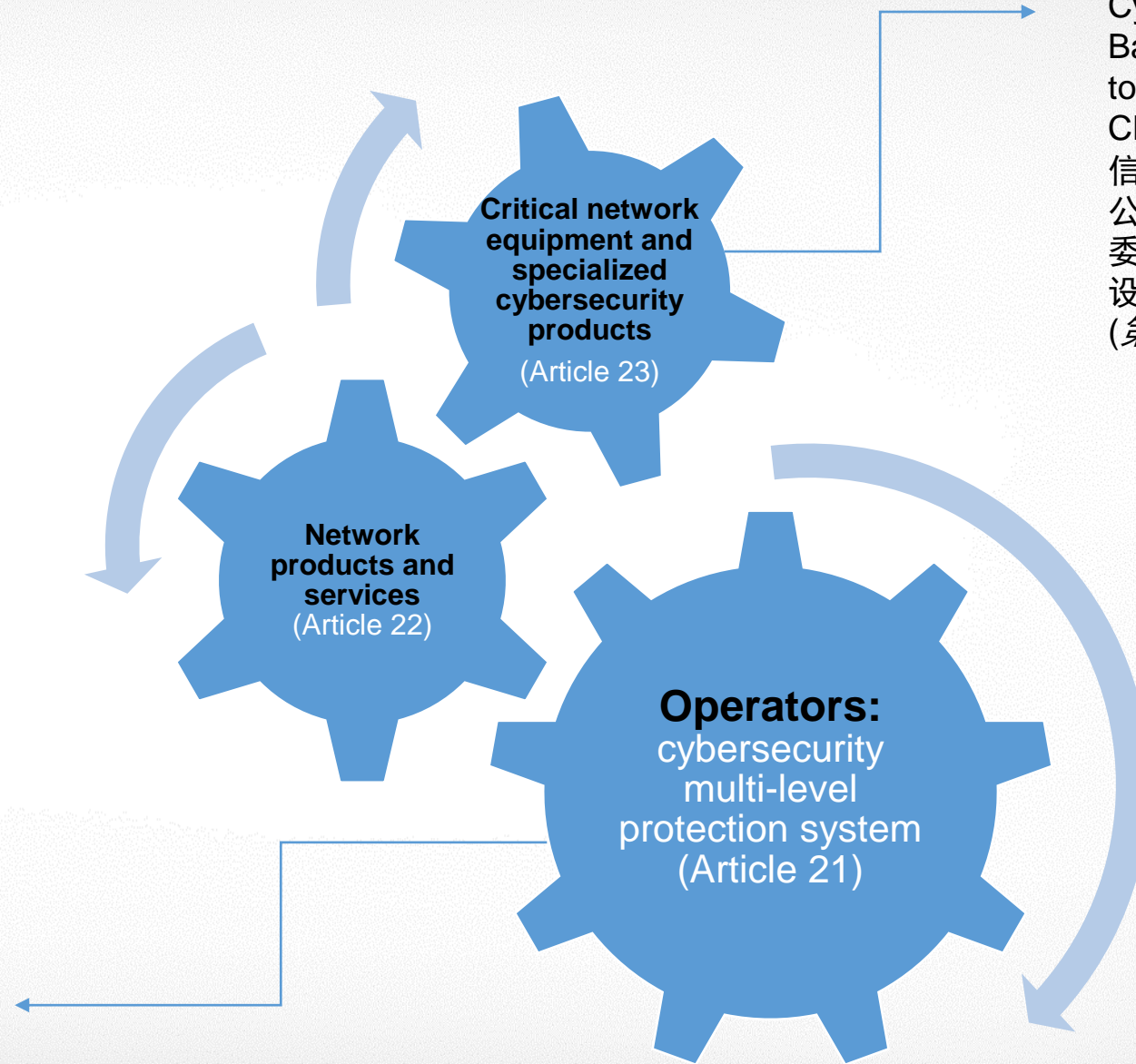
Administrative Measures
for the Security
Protection of Computer
Information Networks
Linked to the Internet

《网络安全法》 (2017)

Cybersecurity Law

Legal Framework on Information Infrastructures

- Catalog of Critical Network Equipment and Specialized Cybersecurity Products (First Batch) developed by CAC, together with MIIT, MPS and CNCA (June 2017) 国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门制定了《网络关键设备和网络安全专用产品目录(第一批)》(2017年6月)

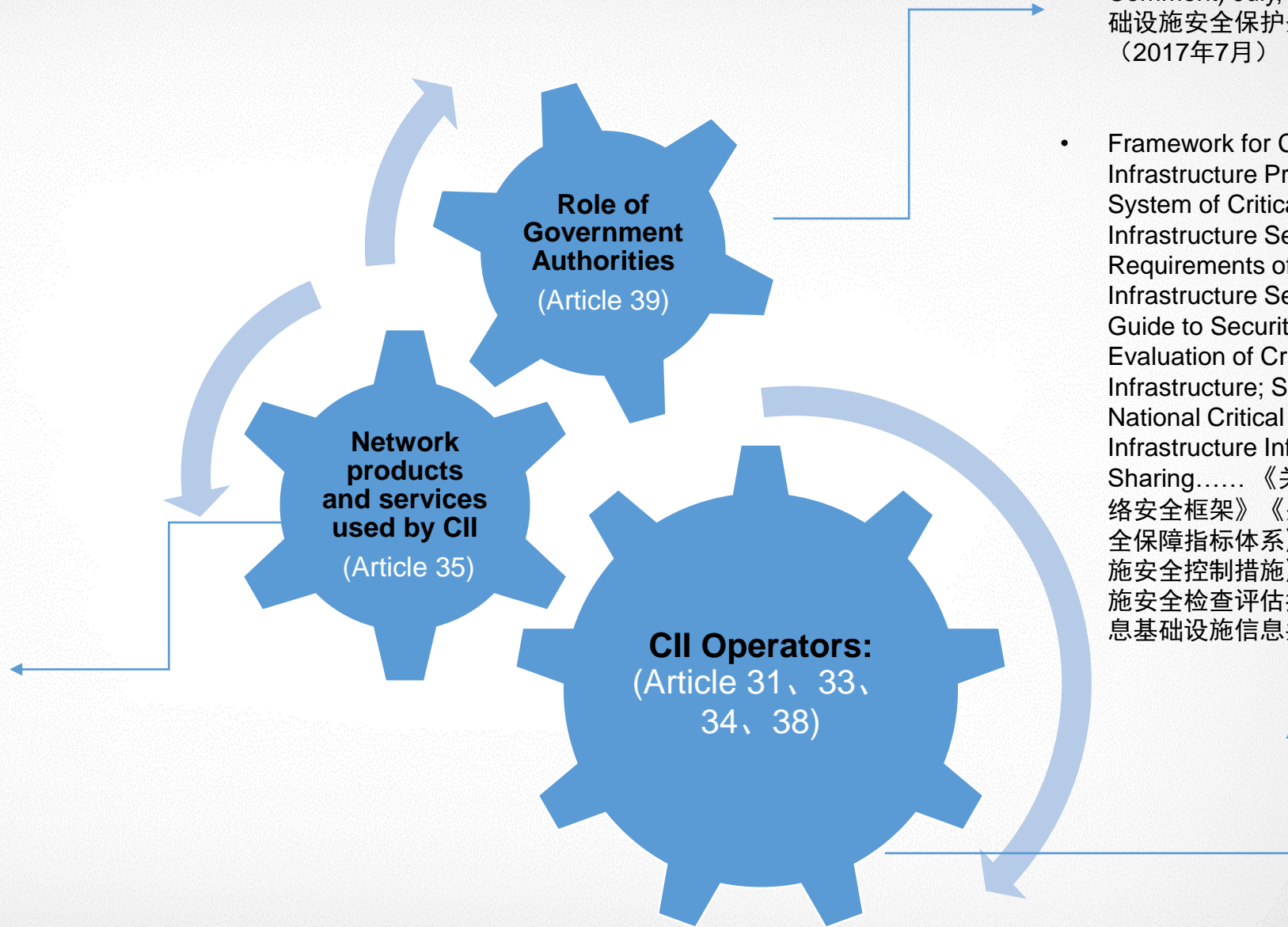


- MPS: Regulations on Cybersecurity Multi-level Protection Scheme (Draft for Comment) June 2018公安部《网络安全等级保护条例(征求意见稿)》(2018年6月)
- Information Security Technology-Baseline for Classified Protection of Cybersecurity; Information Security Technology-Evaluation Requirements for Classified Protection of Cybersecurity; Information Security Technology-Technical Requirements of Security Design for Classified Protection of Cybersecurity. May 2019《信息安全技术网络安全等级保护基本要求》《信息安全技术网络安全等级保护测评要求》《信息安全技术网络安全等级保护安全技术要求》(2019年5月)

Security of Ordinary Network Operators

Legal Framework on Information Infrastructures

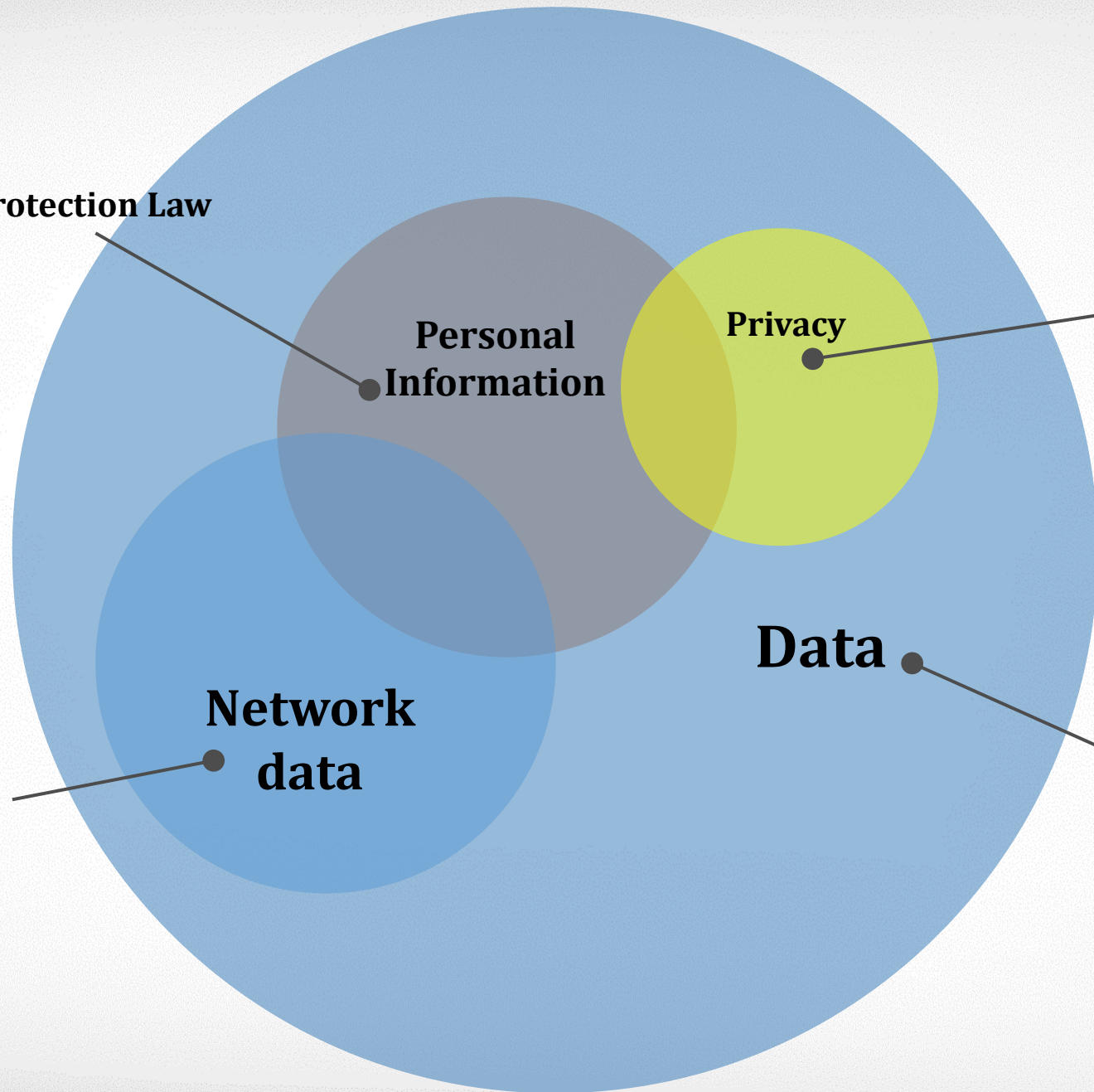
- Measures for Security Review of Network Product and Service (for Trial Implementation) June 2017 《网络产品和服务安全审查办法（试行）》（2017年6月）
- Measures on Cybersecurity Review, April 2020 《网络安全审查办法》（2020年4月）
- Opinions on Strengthening the Security of Cloud Computing Services for Party and Government Departments; December 2014 《关于加强党政部门云计算服务网络安全管理的意见》（2014年12月）



- Critical Information Infrastructure Protection Regulation (Draft for Comment) July, 2017 《关键信息基础设施安全保护条例(征求意见稿)》（2017年7月）
- Framework for Critical Information Infrastructure Protection; Indicator System of Critical Information Infrastructure Security Assurance; Requirements of Critical Information Infrastructure Security Controls; Guide to Security Inspection and Evaluation of Critical Information Infrastructure; Specifications on National Critical Information Infrastructure Information Sharing..... 《关键信息基础设施网络安全框架》《关键信息基础设施安全保障指标体系》《关键信息基础设施安全控制措施》《关键信息基础设施安全检查评估指南》《国家关键信息基础设施信息共享规范》.....

Security of Critical Information Infrastructures

• **Personal Information Protection Law**



**Personal
Information**

Privacy

**Network
data**

Data

• **Civil Code**

• **Data Security Law**


• **Cybersecurity Law**

Main Components of PIPL

General Approaches to Personal Data Protection

Administrative law

- ▶ Cybersecurity Law 2017.6.1
- ▶ Personal Information Protection Law 2021.11.1
- Data Security Law 2021.9.1
- E-Commerce Law 2018.5
- Law of the PRC on the Protection of Consumer Rights and Interests 2013.10



Constitutional Law and Personality rights

Civil law

- ▶ Civil Code 2020.5

Criminal law

- Crimes against Citizens' Personal Information (Amendment IX to the Criminal Law) ▶
- Crime of infringement of freedom of correspondence
- Crime of open, hide, or destroy mail or telegrams without authorization
- Crime of illegal acquisition of computer information system data
- The crime of refusing to fulfill the obligations of information cybersecurity management (Amendment IX to the Criminal Law) ▶

Main Concepts of PIPL

- Personal Data

Personal information is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization handling.

- Processing

Personal information handling includes personal information collection, storage, use, sorting, transmission, provision, disclosure, deletion, etc.

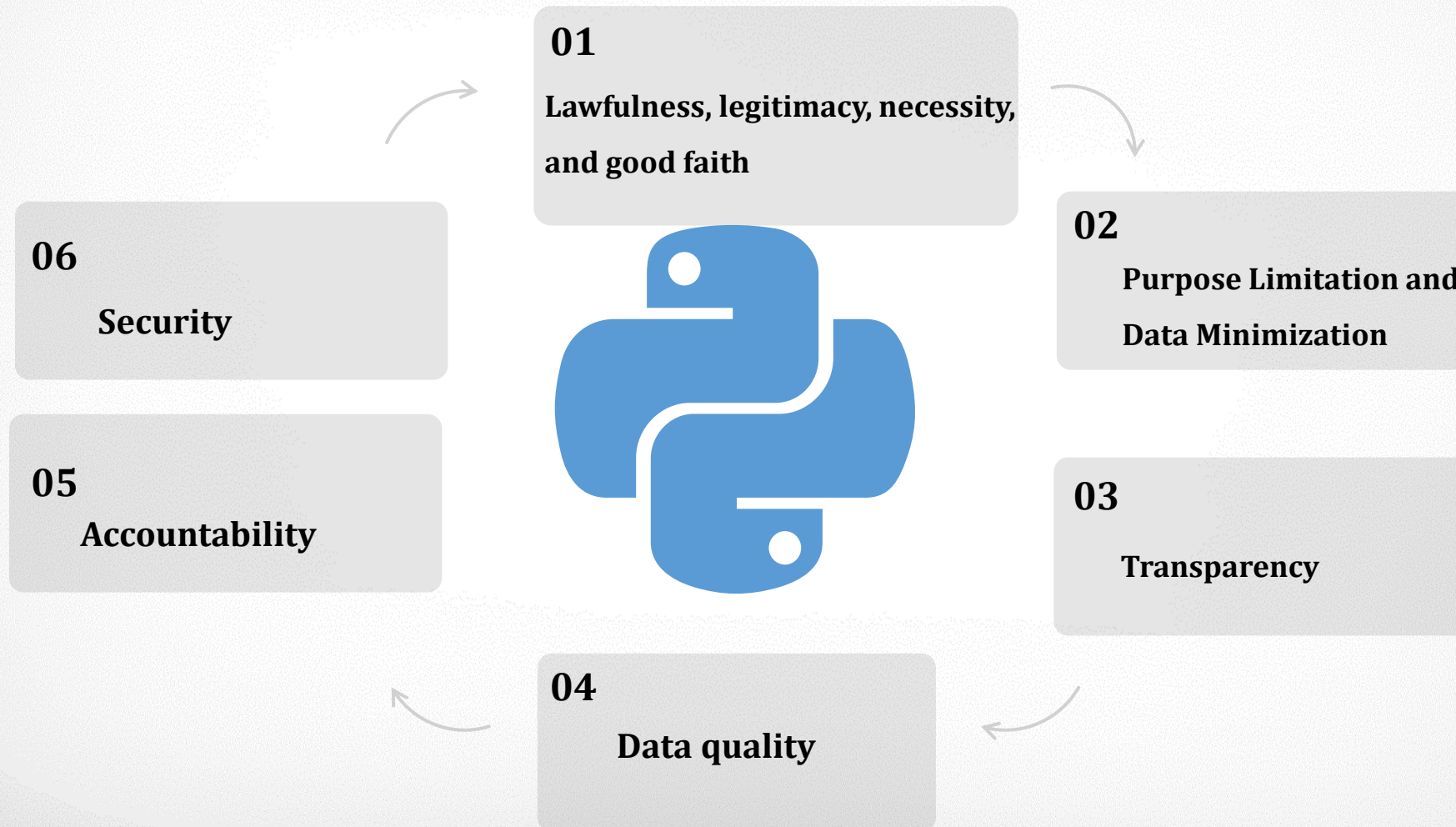
- Personal Data Processor

Personal Data Processor refers to organizations and individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods.

- De-identification

the process of personal information undergoing processing to ensure it is impossible to identify specific natural persons without the support of additional information.

Six principles of PIPL



Main Content of PIPL

Rules

Lawful Processing Grounds

Transparency requirements

Sensitive Information

Interactions with Third Party

Internal Processing

Special protection mechanism

Joint processing

Outsourcing

Sharing

Cross-border transfer

Storage

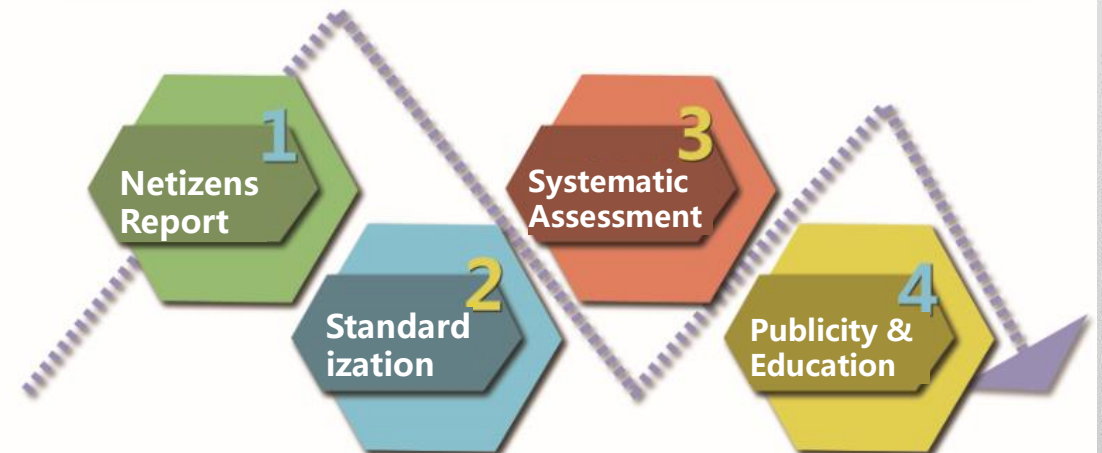
Publicly disclosure

Automated Decision Making

Identification in Public Spaces

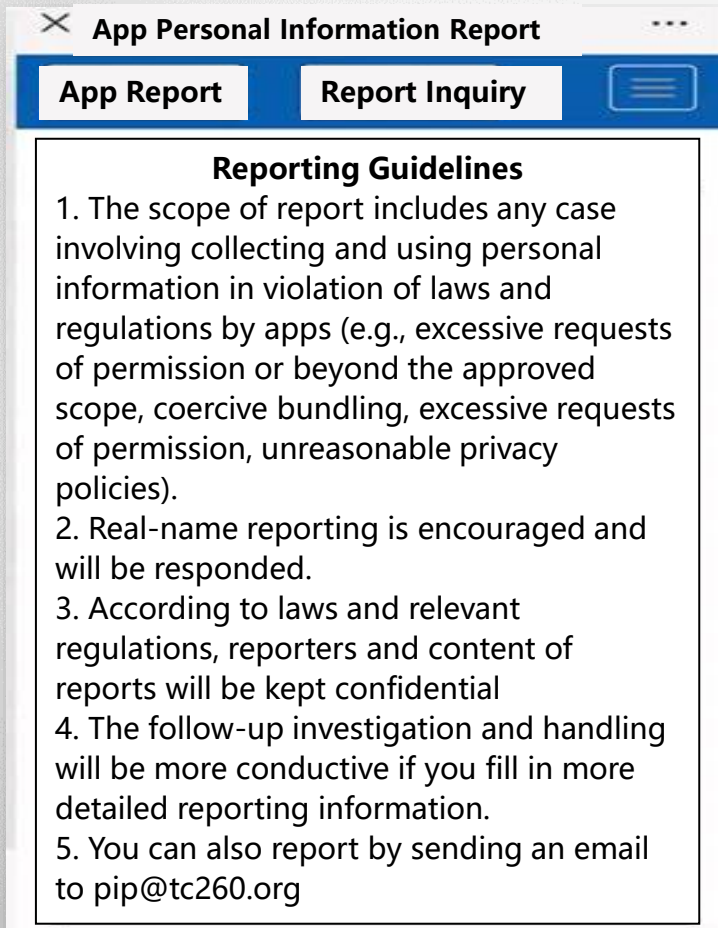
■ Context and Guidelines

To implement *the Cybersecurity Law* and *the Law on the Protection of the Rights and Interests of Consumers*, CAC, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the State Administration of Market Regulation, jointly issued the ***"Announcement on Carrying out Special Campaigns against Apps Collecting and Using Personal Information in Violation of Laws and Regulations"*** and decided to undertake nationwide special campaigns on illegal collection and use of personal information through Apps from January to December 2019.



Netizens Report: Provide Clues for Violations

The App Task Force has set up the "App Personal Information Report" WeChat public account and a special mailbox (pip@tc260.org.cn) to receive reports from netizens regarding the illegal collection and use of personal information by apps.



App Personal Information Report

App Report | Report Inquiry

Reporting Guidelines

1. The scope of report includes any case involving collecting and using personal information in violation of laws and regulations by apps (e.g., excessive requests of permission or beyond the approved scope, coercive bundling, excessive requests of permission, unreasonable privacy policies).
2. Real-name reporting is encouraged and will be responded.
3. According to laws and relevant regulations, reporters and content of reports will be kept confidential
4. The follow-up investigation and handling will be more conducive if you fill in more detailed reporting information.
5. You can also report by sending an email to pip@tc260.org



- In the first year, a total of 8992 reports had been received.
- Including 6172 anonymous and 2820 real-name reports involving 2000+ apps
- 203 reports were received via email
- After verification, nearly 600 app were selected to be included in the assessment scope

Types
of
Problems
Reported



Types of Problems		Number of Reporting
1	Coercive or frequent requests of permissions unrelated to business	3591
2	Collect information unrelated to business beyond the approved scope	3275
3	Unreasonable clauses	3098
4	Bundling business functions by requiring blanket consent from users	2496
5	Absence of app privacy policy	2284
6	Unable to erase or rectify personal information	2257
7	Unable to cancel accounts	2042
8	Harassment of address book friends	1512
9	Lack of complaint channel or invalid channel	1045
10	Other	337

■ Standardization: Refine the Requirements of Laws and Regulations

First, revise the national standard *GB/T 35273 "Personal Information Security Specification"* to **specify the detailed requirements for the basic principle of "legality, propriety and necessity"** set forth in the PIPL Law.

Second, formulate *the Basic Specification for Collecting Personal Information in Mobile Internet Applications (App)(Draft for Comments)* to **clarify the scope of "necessary information and permissions" collected by apps.**

Third, formulate *the Measures for the Ascertainment of Illegal Collection and Use of Personal Information through Apps* to **clearly define the illegal activities in App's collection and use of personal information and provide reference for assessment and disposal.**

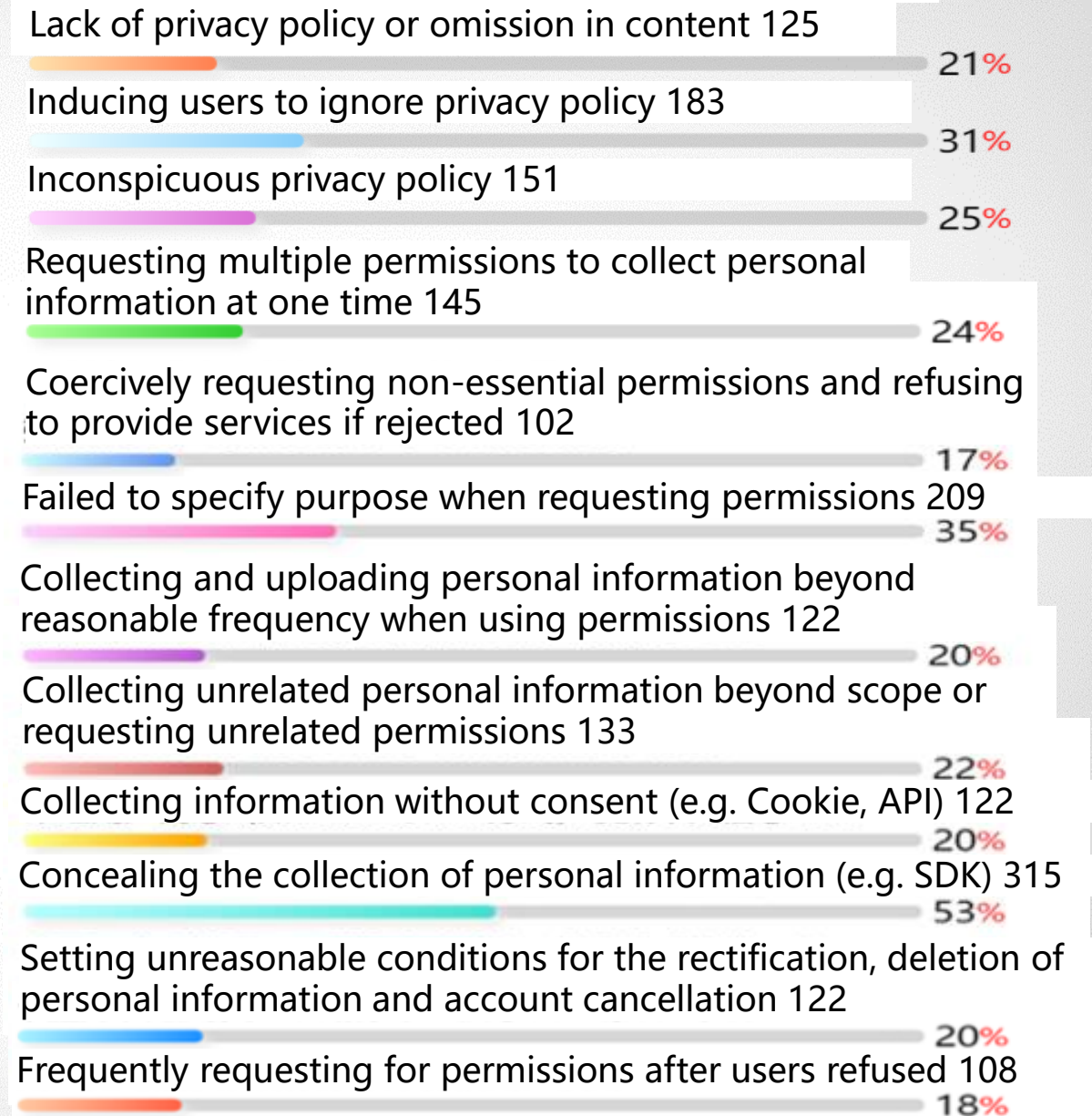
Fourth, publish the *Self-assessment Guide for Illegal Collection and Use of Personal Information through Apps* **as a reference for companies to conduct self-examination and self-correction.**

■ Systematic Assessment: Urge Rectification

Collaborating with more than a dozen professional and technical assessment organizations to carry out systematic assessment of apps on agreement text, user experience and technical testing.

Up to now, the App Task Force has assessed over **600 apps**, and has informed **200 app operators** with large number of users and serious problems of the assessment results, suggesting that they make timely rectification of the **800+ problems** revealed.

Typical Problems Found in Assessments



Publicity and Education: Promoting Citizens' Awareness



Technical details of the offending App were exposed at the “CCTV 3.15 Evening” , and the work progress, evaluation results and interpretation of the App's personal information protection issues were introduced through mainstream media such as Xinhua News Agency, People's Daily, China Central Television and Global Times, which attracted massive attention and **became one of the most searched hashtags in Weibo and other media**. It has been read more than 100 million times.



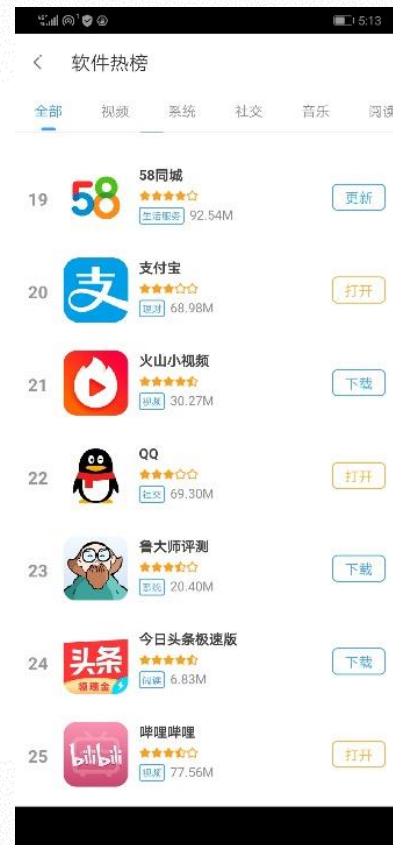
Through the WeChat public account "App Personal Information Report", **a series of articles are published to communicate key personal information protection knowledge** and popularize such knowledge and skills to the public. So far, the WeChat public account has attracted more than 20,000 users, publishing 13 articles with a total reading of 200,000.

Work Achievement I: Assessment covers Mainstream APP Commonly Used by Netizens

The Task Force has completed the assessment of nearly 600 apps, covering the **300 apps** commonly used by netizens with the largest amount of downloads (up to **30 billion** downloads in total).

It involves 16 areas such as online shopping, instant messaging, map navigation, online car booking, news and information, online payment, express delivery and so on, **covering major aspects of netizen life.**

Through urging industry-leading App operators to make rectification, the industry's personal information security level has been effectively improved, and netizens' personal information security has been guarded.



■ Work Achievement II: Established Real-time Communication Mechanisms

At present, **80%** of App operators in **the top 500 download rankings** have established a daily communication mechanism with the Task Force on Apps to realize real-time feedback and communication on compliance issues, user complaints, rectification plans, effect evaluation, etc.

Before launching new products and services, these App operators often communicate with the task force and consult on the personal information security protection plan to prevent problems.

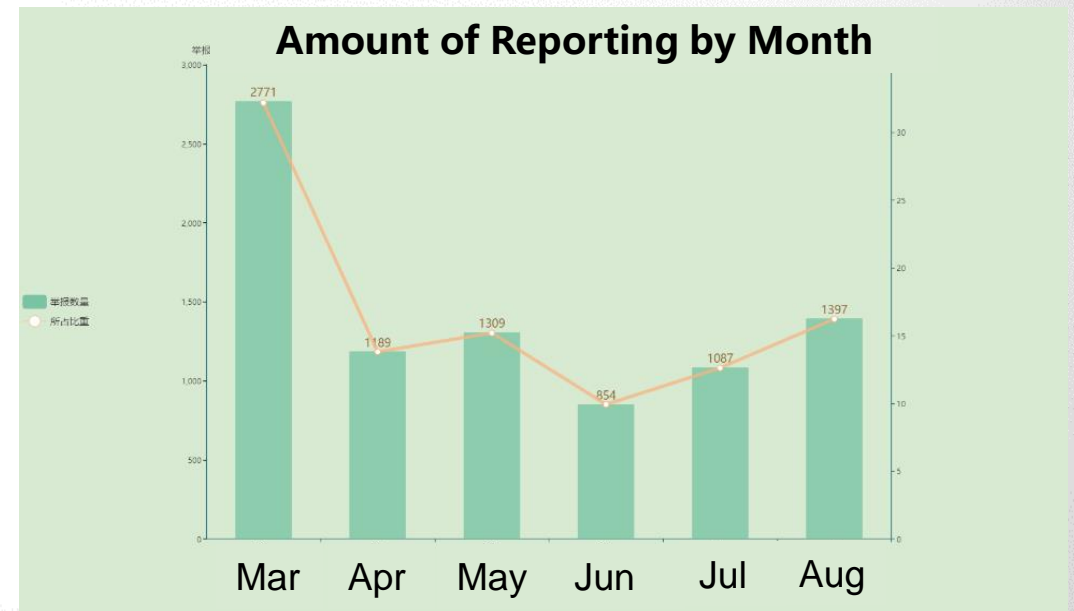


■ Work Achievement III: Positive Leading Effect from Typical Demonstration

In addition to the App included in the assessment, many App operators follow the example of the leading Apps and correct their illegal collection and use spontaneously.

Problems such as lack of privacy policy, requiring users to consent on opening multiple permissions to collect personal information at one time, coercively requesting irrelevant permissions such as address book and location, collecting personal information without users' consent, lack of channels to cancel accounts, lack of communication and compliant channels concerning personal information protection have been significantly improved.

Over the past two months, the number of effective reports from Internet users has **dropped 40%** as compared to the beginning of the year.



Work Achievement IV : Increased Attention on Personal Information Protection

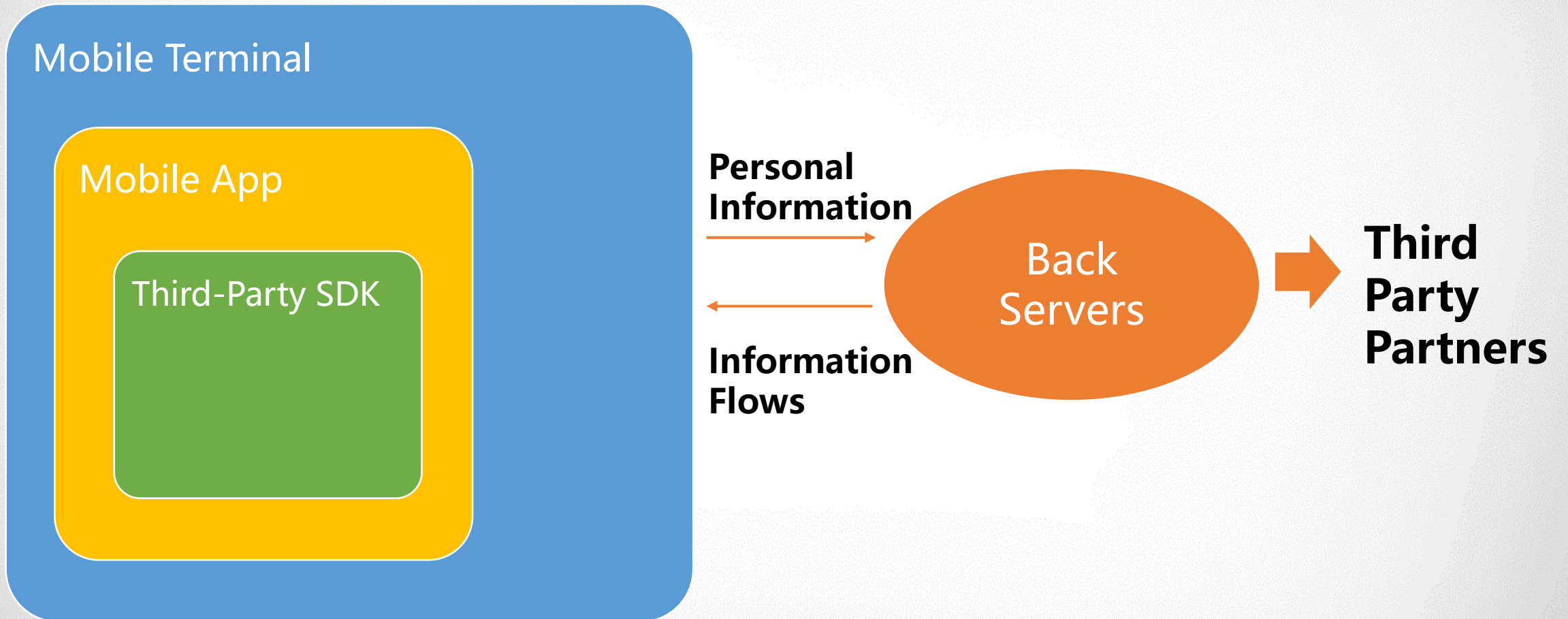
Take Baidu's search results as an example. Currently, there are **4.77 million** ordinary web pages and **358,000** information pages that contain the keyword " Personal Information Protection Task Force on Apps ".

There are **22.54 million** web pages and **1.32 million** information pages with the four standard specifications compiled by the Task Force on Apps as key words.

Organizations, media and citizens have taken the initiative to reveal personal information security problems on apps and carry out supervision by society and public opinion.

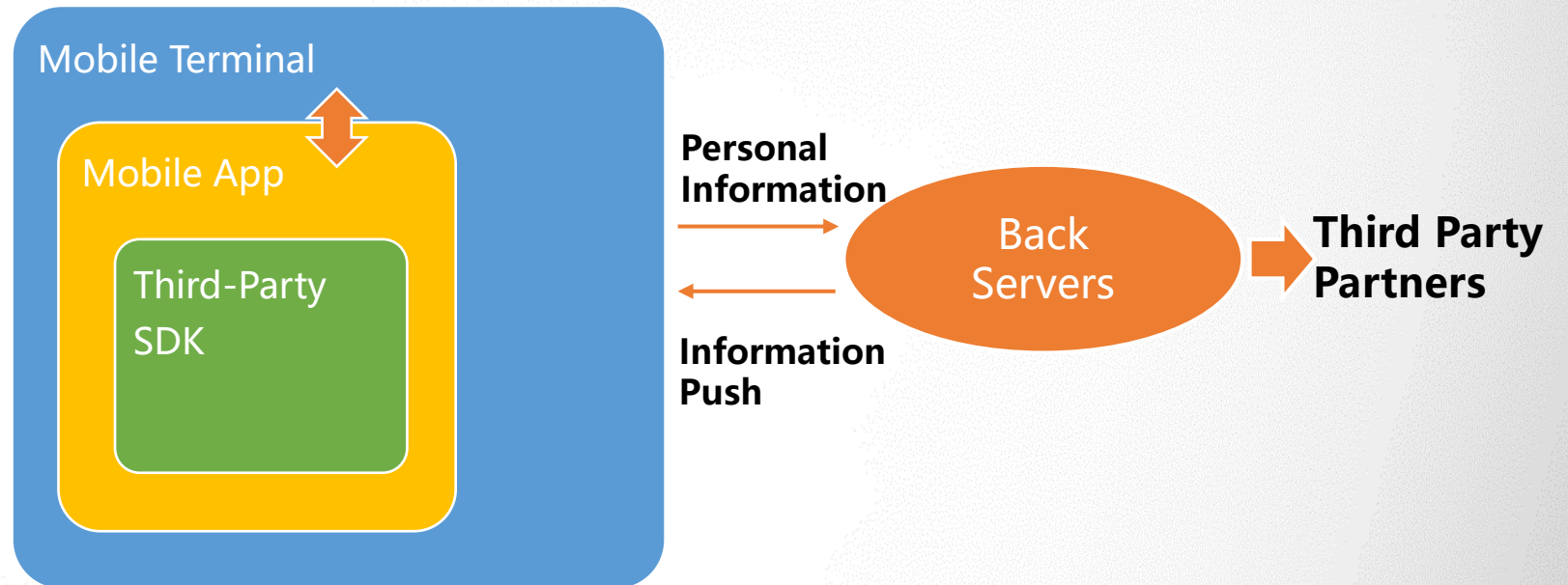


■ Analysis of Mobile App Personal Information Protection



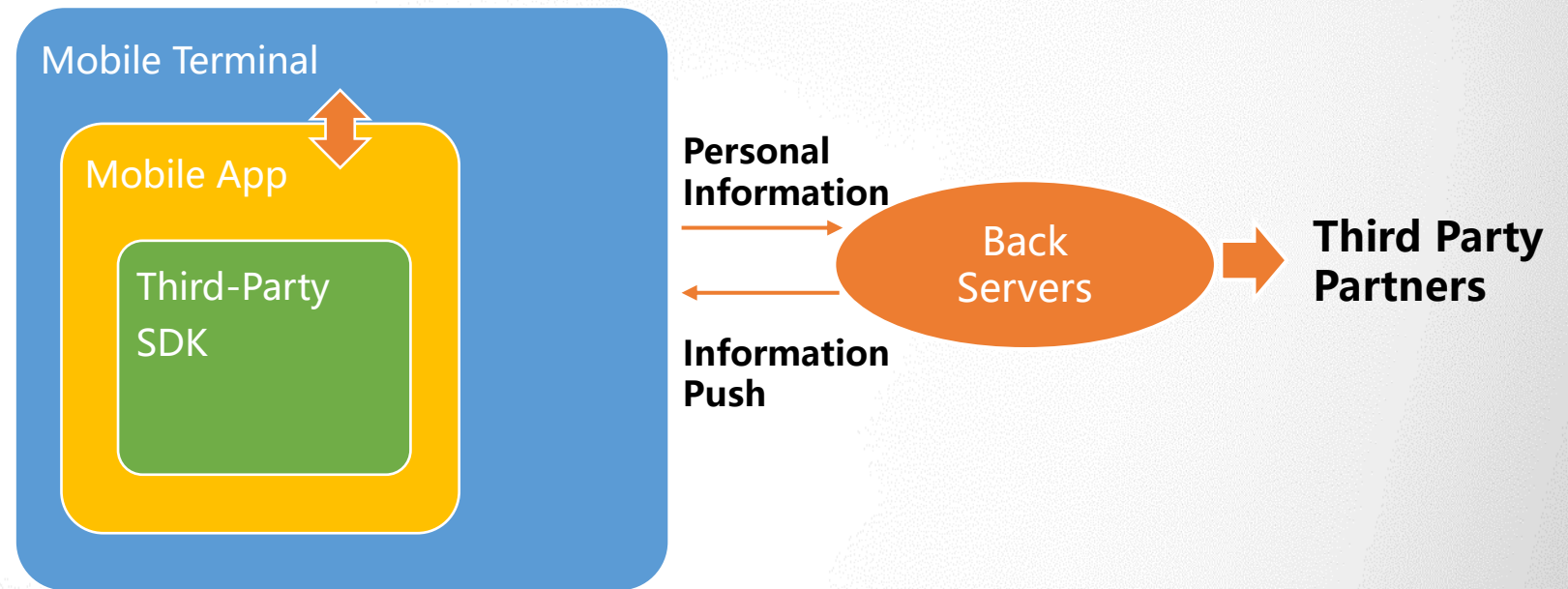
■ Automated Monitoring Indicator I: Permission Declaration and Usage

Item	Content
P1	Number of permissions declared statically by App to collect personal information
P2	Number of permissions that can be retrieved to collect personal information during App operation



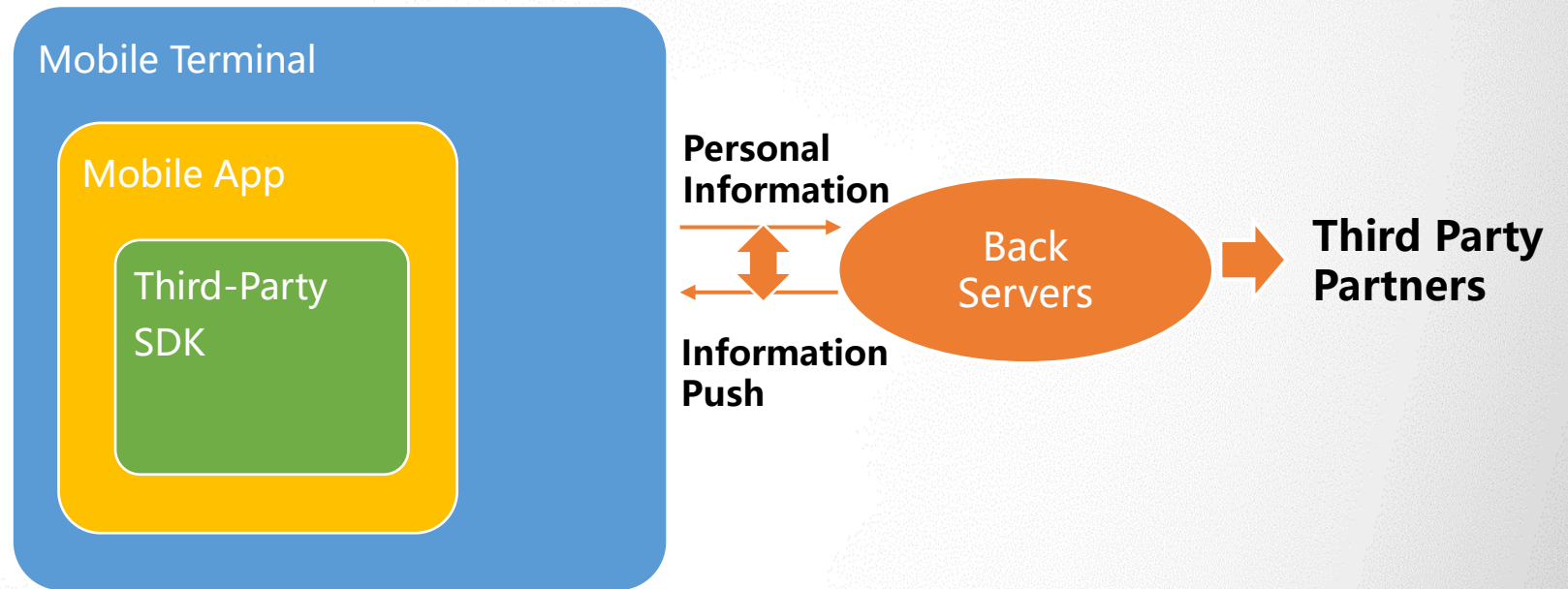
■ Automated Monitoring Indicator II: Frequency of Personal Information Collection

Item	Content
F1	Frequency of reading IMEI/IMSI number
F2	Frequency of reading mobile phone number
F3	Frequency of reading installed applications list
F4	Frequency of reading positioning information
F5	Frequency of reading address book



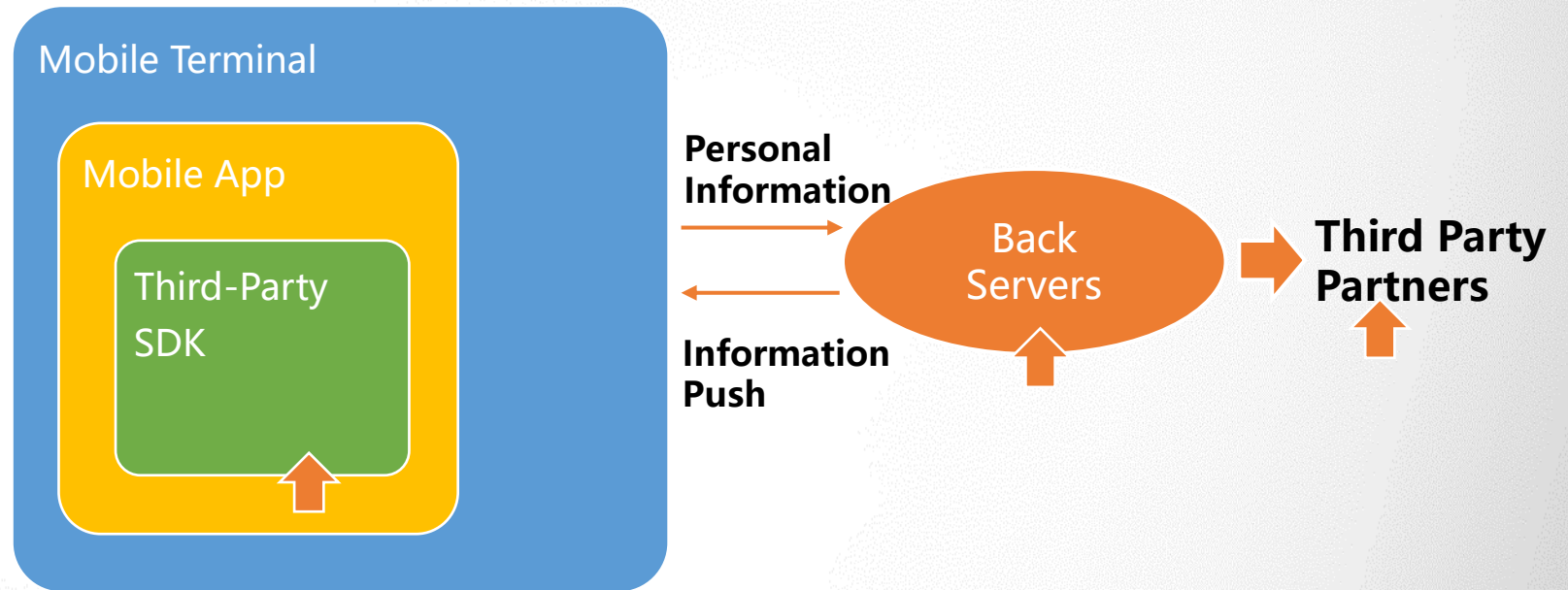
■ Automated Monitoring Indicator III: Network Flow Consumed

Item	Content
N1	Upstream flow in foreground silent state
N2	Upstream flow in background operation state



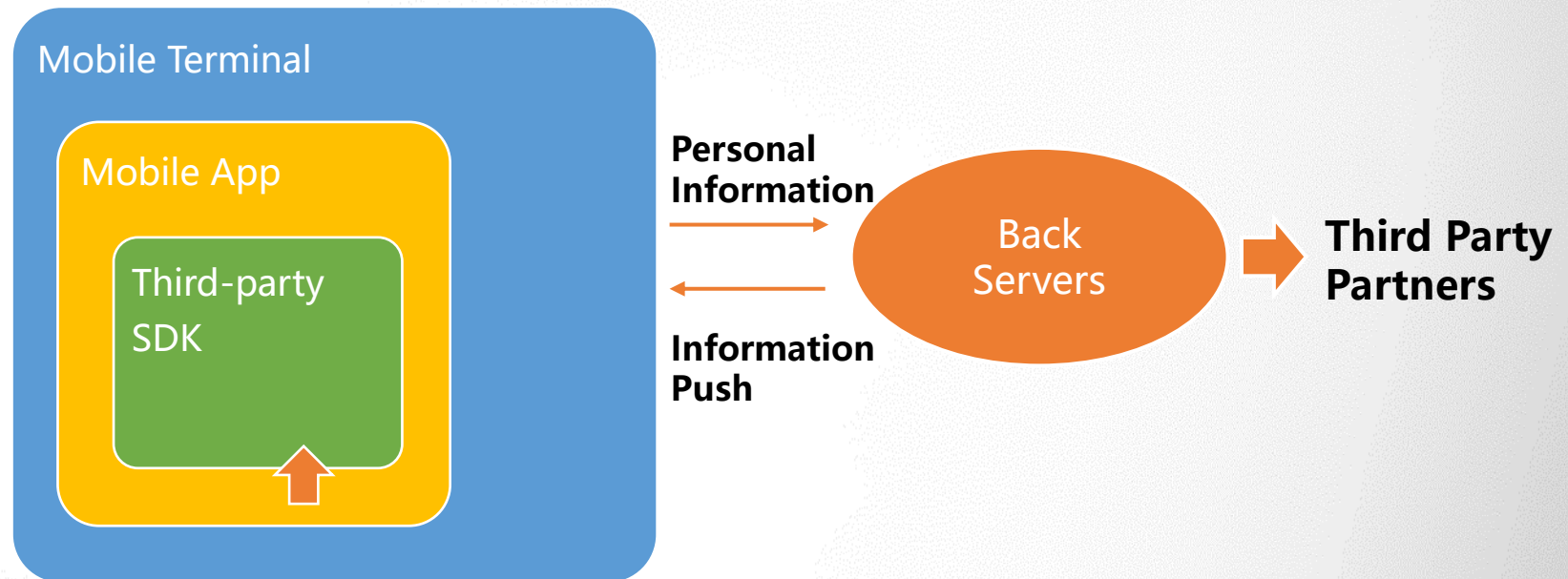
Automated Monitoring Indicator IV: Number of Communication IP and Geographic Locations of IP

Item	Content
I1	Number of domestic IP communications
I2	Number of IP communications with overseas countries



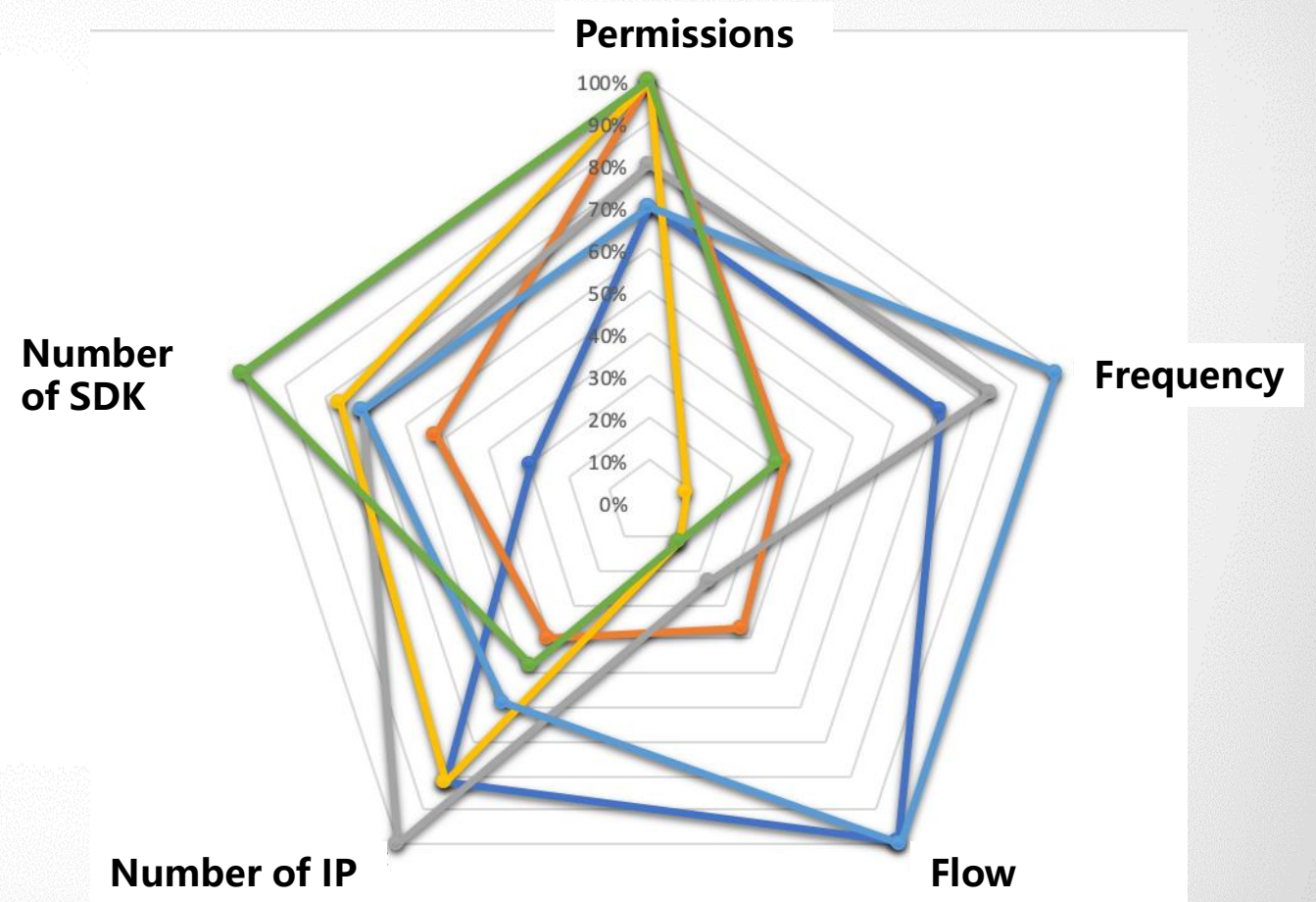
■ Automated Monitoring Indicator V: Number of Third-party SDK Embedded

Item	Content
S1	Number of Third-party SDK Embedded



■ Automated Monitoring Indicator System: Automated Initial Screening of Suspected Apps

The sub-item detection results of the five detection items are combined through algorithm. The final detection result can be embodied in a radar chart with five angles as shown on the right:



■ Next Step: Explore Long-term Supervision Mechanism on Apps

- Improve standards and norms: implement principles and requirements of laws and regulations.
- Improve detection technology, grasp the situation and trend of unlawful acts.
- Expand the scope of assessment to cover all aspects of work and life.
- Promote publicity and education, promote industry self-discipline and social supervision

Thank you for your attention