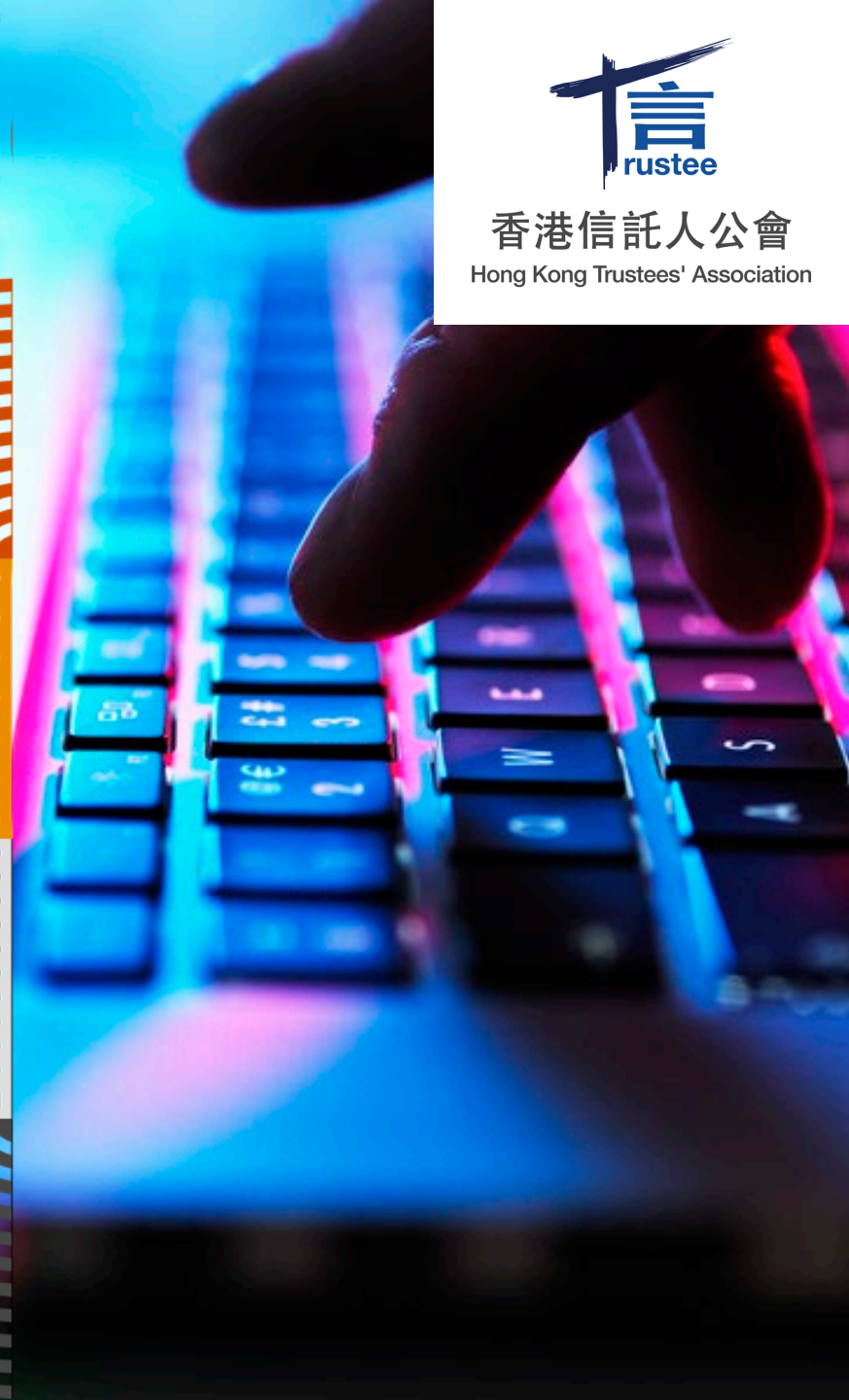
New China Regulations on Cross-Border Personal Data Transfer



香港信託人公會
Hong Kong Trustees' Association

pwc

Tiang & Partners
程偉賓律師事務所

Chiang Ling Li（李江陵）

Chiang Ling Li
Partner
Tiang & Partners

Contact
+852 2833 4938
chiang.ling.li@
tiangandpartners.com

Profile

Chiang Ling Li's practice has focused on Data, Cybersecurity, and Intellectual Proper law since 1994. She has been in the forefront of the law, having obtained approvals for outbound transfer of human genetic data as well as handled data breaches and other cyber crisis for multinational companies.

Chiang recently assisted a Asian government authority with the data issues relating to the establishment of a data stock exchange, advised a Middle Eastern government on putting in place a cybersecurity and data regulatory framework for that country, assisted with the legal analysis relating to possible free flow of data within the Greater Bay Area (GBA), defended a major Hong Kong health group before the Hong Kong data regulator, proceeded with security assessment by China data regulator for outbound transfer of data for multinational companies, advised a global law firm on data protection issues, advised a US alliance on data vulnerability issues, and assisted a quasi government authority and an university to put in place data governance frameworks for the data from multiple jurisdictions (including the UK, Germany, France, China, Taiwan, Korea, Singapore, Australia, Japan, Canada and the US).

Areas of expertise

- Cybersecurity and data protection
- Pharmaceutical and medical devices
- Technology
- Intellectual property
- Litigation and arbitration

** included matters handled prior to joining Tiang & Partners.*

Accolades

Chiang Ling Li is ranked as a leading lawyer in Intellectual Property (International Firms) in China

Chambers Greater China Region, 2023

Tiang & Partners is ranked as a Firm to Watch in Intellectual Property in Hong Kong

Legal 500 Asia Pacific, 2023

Chiang Ling Li is ranked as a Leading Individual in Enforcement & Litigation, Prosecution & Strategy, and Transactions

World Trademark Review 1000, 2023

Tiang & Partners is ranked in Trademarks / Copyright and Patents (Tier 1 for Patents)

Asian Legal Business (ALB) IP Rankings, 2022

Chiang Ling Li is ranked as a Leading Individual in Patent: Litigation

IAM Patent 1000, 2022

Chiang Ling Li is recommended in “IP Star” in both Patent and Trade Mark

Managing IP, 2022

Chiang Ling Li is recognised as a IP Expert in Patents, Trademarks, IP Litigation

Asia IP, 2023

Accolades

Chambers RANKED IN Greater China Region 2023	WTR 1000 World Trademark Review	AsiaIP INFORMED ANALYSIS	ASIAN LEGAL BUSINESS ALB	MIP IP STARS	IAM 1000
Chiang Ling Li is ranked as a leading lawyer in Intellectual Property (International Firms) in China *Chambers Greater China Region, Global* 2023	Chiang Ling Li is ranked as a Leading Individual in Prosecution & Strategy, and Transactions *World Trademark Review 1000,* 2023	Chiang Ling Li is recognised as a IP Expert in Patents, Trademarks, IP Litigation *Asia IP,* 2023	Tiang & Partners is ranked in Trademarks / Copyright and Patents (Tier 1 for Patents) *Asian Legal Business (ALB)* IP Rankings, 2022	Chiang Ling Li is recommended in “IP Star” in both Patent and Trade Mark *Managing IP*, 2022	Chiang Ling Li is ranked as a Leading Individual in Patent: Litigation *IAM Patent 1000,* 2022

Quick Backgrounds

China Cybersecurity/Data Privacy Laws include

- ***China's Cybersecurity Law*** *("CSL" effective June 1, 2017)*
- People's Bank of China Directive
- *Information Security Technology—Implementation Guide for Classified Protection of Information System (GB/T 25058-2019), Information Security Technology—Classification Guide for Classified Protection of Cybersecurity (GB/T 22240-2020)*, *Information Security Technology—Basic Requirements for Cybersecurity Protection of Critical Information Infrastructure (GB/T 39204-2020)*, *Information Security Technology—Personal Information Security Specification (GB/T 35273-2020)*, Financial Personal Information Standard JR/T 0171-2020. etc.
- *Tort Law*
- *Measures for Cybersecurity Review*
- *Notice of the Ministry of Industry and Information Technology on Cleaning Up and Regulating the Internet Access Service Market*
- *Provisions on Internet Security Supervision and Inspection by Public Security Organs*
- *Cloud Computing Services Security Assessment Measures*
- *Regulation for the Cybersecurity Protection of Personal Information of Minors*
- *Civil Code*
- *Judicial Interpretation on Application of Law in the Trial of Civil Cases Relating to the Use of Facial Recognition Technologies*
- *Regulations on the Security and Protection of Critical Information Infrastructure*
- ***Data Security Law*** *("DSL" effective Sept 1, 2021)*
- ***Personal Information Protection Law*** *("PIPL" effective Nov 1, 2021)*

Definitions

- ✓ **Important Data: data that may endanger national security, economic operation, social stability, public health, and safety once they are tampered with, destroyed, leaked, or illegally obtained or used illegally**

- ✓ **Sensitive Personal Information: personal information that, once leaked or illegally used, can easily lead to the infringement of personal dignity of natural persons or the harm on personal and property safety, including biometrics, religious beliefs, specific identities, medical health, financial accounts, whereabouts, and other information, as well as the personal information of minors under the age of 14**
- ✓ **Critical Information Infrastructure ("CII"): important network facilities and information systems in the industries of public communication and information services, energy, transportation, water conservancy, finance, public services, e-government, national defence, science and technology as well as those that may seriously endanger national security, national economy and the people's livelihood, and public interests in case of damage, loss of function or data leakage. Industry regulators are responsible for giving guidance and issuing detailed catalogues of CIIs within their own industries.**
- ✓ **Outbound Transfer/Cross-border Transfer: transfer and access, including remote access**

Application

China Personal Information Protection Law applies to:

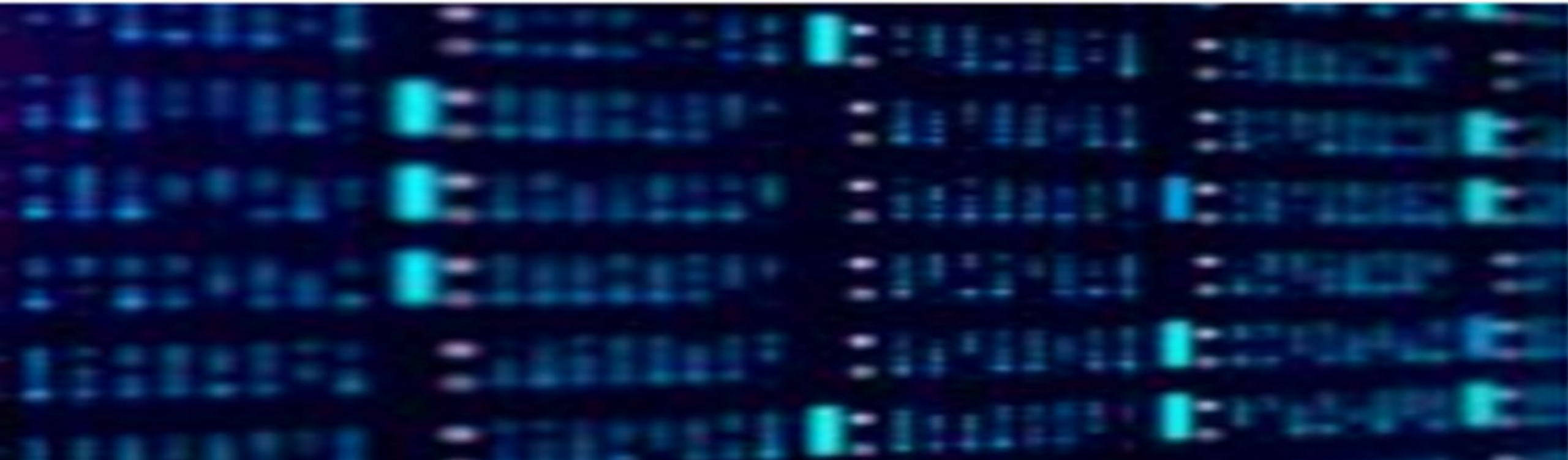
- foreign companies operating in China

- certain activities of foreign companies NOT operating in China
  - if foreign company:
    - sells products or provides services to individuals in China, e.g. through CBEC or e-commerce; or
    - analyzes the buying habits or other activities of individuals in China
  - Besides fines, damages and criminal actions, PIPL expressly provides that retaliation measures may be taken against foreign offenders

New Outbound Personal Data Transfer Rules

Outbound transfer of personal data from the Mainland

- Must use 1 of the following 3 permissible mechanisms ：
  - pass security assessment (obtain government approval)
  - obtain certification by certification organization designated by regulator
  - enter into standard contract (Chinese SCCs) with overseas recipient



Chinese government approval is needed for following outbound transfers:

- ✓ Transfer of personal data collected or generated in China by a CII Operator
- ✓ Transfer of important data by any organization
- ✓ Transfer of personal or other data by a Chinese organization or individual to a foreign law enforcement or judicial body
- ✓ Transfer of personal data by data controller who processes personal data of ≥ 1 million people
- ✓ Transfer of personal data by data controller who has since 1 January of the preceding year cumulatively provided personal data of 100,000 individuals or sensitive personal data of 10,000 individuals outside of China

If government approval is not needed, outbound transfer of personal data may proceed using 1 of the below prescribed mechanisms:

1. Certification by professional institution designated by Chinese government
2. Entering into standard contract ("Chinese SCCs") of Chinese government with overseas recipient

Additional Requirements:

- Necessity
- Impact assessment and 3 years' record retention
- Giving notice to the individual of all of the following:
  - name and contact information of overseas recipient
  - purpose and method of processing
  - type of personal information
  - process for how individual may exercise rights
- Separate Consent

Government Approval (Security Assessment)

Government Approval (Security Assessment)

- CSL, DSL and PIPL: transfer of certain data outside of Mainland China requires prior Chinese government approval ("security assessment")
- Consent of the individual not sufficient
- *Measures on Security Assessment of Cross-border Data Transfer* governing security assessment process, effective 1 September 2022, and Guidelines for applying for security assessment for cross-border transfer of personal information
- Any non-compliant transfer of data outside of China must be rectified by 1 March 2023

Government Approval (Security Assessment) (cont'd)

When is security assessment required?

- CII Operator transfers personal data outside of China
- Data controller who processes personal information of one million people or above transfers personal data outside China
- Data controller transfers "important data" outside of China
- Data controller who has since 1 January of the preceding year:
  - cumulatively provided personal information of 100,000 individuals outside of China or
  - cumulatively provided sensitive personal information of 10,000 individuals outside of China

  transfers personal data outside of China
- Other situations as prescribed by CAC

Government Approval (Security Assessment) (cont'd)

Security assessment process

- Before applying for a security assessment, conduct self-assessment
- Self-assessment to evaluate issues including (i) the data to be transferred and the necessity of the transfer; (ii) the overseas recipient, (iii) the sufficiency of legal protection provided by the contract with the overseas recipient, and (iv) the risk of data leakage
- Submit through provincial CAC for approval by national CAC
- Submit (i) the report of the self-assessment; (ii) the application form; (iii) the legal documents between the data controller and the overseas recipient; etc.

Government Approval (Security Assessment) (cont'd)

Cross-border data transfer contract

- Application for government approval should include agreement between data controller and overseas recipient
- Agreement sets out the purpose, method and scope of the data transfer, the manner of overseas storage of data, the obligations and liabilities of the overseas recipient, the dispute resolution mechanism, etc.
- Overseas recipient to take safety measures when there are force majeure events or changes in the data security regulation in the foreign location
- Parties should pass the security assessment before signing contracts, or parties should provide that their contracts are subject to the security assessment

Government Approval (Security Assessment) (cont'd)

Government security assessment timeline

01 Upon the receipt of application, the provincial CAC would assess whether the materials and information are sufficient within 5 business days

02 Provincial CAC would pass the application to the national CAC if application materials and information are sufficient

03 National CAC would inform whether the application is accepted within 7 business days

04 National CAC would complete the security assessment within 45 business days (unless extension required for complicated situations)

The above timeline does not include the time for self-assessment

Government Approval (Security Assessment) (cont'd)

Validity of security assessment

- Each security assessment is valid for two years
- In case of significant change, reapplication for approval
- Approval renewal to be submitted at least 60 business days before the expiry of validity period

Certification of Cross-border Data Transfer

Certification of Cross-border Data Transfer

- Certification of cross-border data transfer by designated organisations can be used as a mechanism for cross-border data transfers from China
- Guidelines set out in regulation (Implementation Rules for Personal Information Protection Certification) and standard (Specifications for security certification of cross-border processing of personal information（V2.0-202212）)
- Certification organizations should be designated by Chinese government as the next step
- Certification must involve on-site inspection by the certification organization
- Initial validity of a certification is three years; the certification organization is to monitor during the validity period

Certification of Cross-border Data Transfer (cont'd)

01 Agreement

- Agreement between the data controller and overseas recipient
- Agreement covering details of the cross-border processing activities
- Overseas recipient undertakes to accept the supervision by the certification organisation and to be bound by relevant China law
- Individual is a third party beneficiary

02 Organisation Management

- Both data controller and overseas recipient must:
  - ❑ Appoint DPOs
  - ❑ Set up organisation structures which handle data related works such as handling data access requests and complaints and conducting data compliance audits
  - ❑ Record data processing activities and maintain records for at least three years
  - ❑ Prompt report to Chinese regulators of breaches and possible breaches, and, in accordance with the law, notice to the individual

Certification of Cross-border Data Transfer (cont'd)

03 Personal Information Processing Rules

- Both the data controller and overseas recipient to comply with the same set of personal information processing rules
- Rules to cover the manner of handling personal data, the duration of data retention, the permissible locations for onward transfer of the data, etc.
- Specify outbound transfer jurisdictions

04 Impact Assessment

- Before cross-border personal data transfer may proceed, an impact assessment to be conducted
- Assessment must evaluate legality of data transfer, whether the protection measures are compatible with the risk levels, whether the individual's right will be undermined, etc.

05 Individual's Right

- Individuals have the right of information, right to withdraw consent, and right to access
- Individuals have the right to require a copy of the relevant part of the agreement between the data controller and overseas recipient
- Individuals have the right to reject automated decision making
- Individuals have the right to complain to Chinese regulators and sue in China

Chinese SCCs

Chinese SCCs

- Chinese SCCs can be used as a mechanism for cross-border data transfers from Mainland China
- Chinese SCCs are provisions to be entered into by data controllers and overseas recipients, governing the rights and liabilities of the parties as well as the individuals
- Contracts between data controllers and overseas recipients concerning the cross-border transfer of personal information may not conflict with Chinese SCCs

Chinese SCCs (cont'd)

Who may rely on Chinese SCCs for outbound transfer of personal data outside of China?

Data controllers meeting all of the following conditions:

(1) It is not a CIIO

(2) It processes personal information of less than one (1) million individuals

(3) It has not cumulatively provided overseas personal information of 100,000 individuals since 1 January of the preceding year

(4) It has not cumulatively provided overseas sensitive personal information of 10,000 individuals since 1 January of the preceding year

Chinese SCCs (cont'd)

Impact assessment and recordal

- Impact assessment and 3 years' record retention
- Impact assessment submission to provincial CAC within 10 working days from effective date of Chinese SCCs
- Chinese SCCs submission to provincial CAC within 10 working days from effective date of Chinese SCCs
- Chinese SCCs to be re-executed and re-recorded in case of substantive change

Chinese SCCs (cont'd)

Rights of individuals

- Individual to be notified of him/her being a third party beneficiary under Chinese SCCs
- Chinese SCCs to be provided to the individual upon request
- Other requirements including:
  - automated decision making
  - transparency (the data controller and the overseas recipient needing to explain the rules of data processing to the individual); communications with the individual being clear, easy to understand and thorough
  - right to access, copy, amend and delete his/her data
  - right to be given reasons of non-compliance and informed of complaint and litigation options

Chinese SCCs (cont'd)

Obligations of overseas recipient

- Overseas recipient subject to the supervision of Chinese regulators (including complying with their orders and providing written proof of having taken compliance steps)
- Overseas recipient must keep records of its data processing for at least three (3) years

Onward transfer

- Must comply with additional requirements, including
  - Necessity
  - Separate Consent

Chinese SCCs (cont'd)

Country risk assessment

- Whether overseas jurisdiction accords a level of protection essentially equivalent to that required by China law
- Data controller and overseas recipient need to conduct prior assessment of the law and enforcement in overseas jurisdiction

Contact person

- Overseas recipient should designate an internal contact for addressing inquiries and complaints from the individuals
- Contact details should be notified to the individuals

Chinese SCCs (cont'd)

Governing law and dispute resolution

- Data controller and overseas recipient
  - China governing law
  - Arbitration (China arbitration or New York Convention)
  - Litigation (Chinese court).

- The individual
  - Chinese regulators
  - Chinese litigation
  - Data controller and overseas recipient are jointly liable

Liabilities for Non-compliance

Liabilities

- Confiscation of income
- Fine up to RMB 50 million or 5% of turnover of the previous year
- Business suspension
- Revocation of business licenses
- Violations recorded into the “credit files”
- Individuals fined up to RMB 1 million + blacklisting
- Damages (reverse burden of proof)
- Criminal prosecution

List of APPs penalized on the grounds of violation of PIPL, CSL, etc.

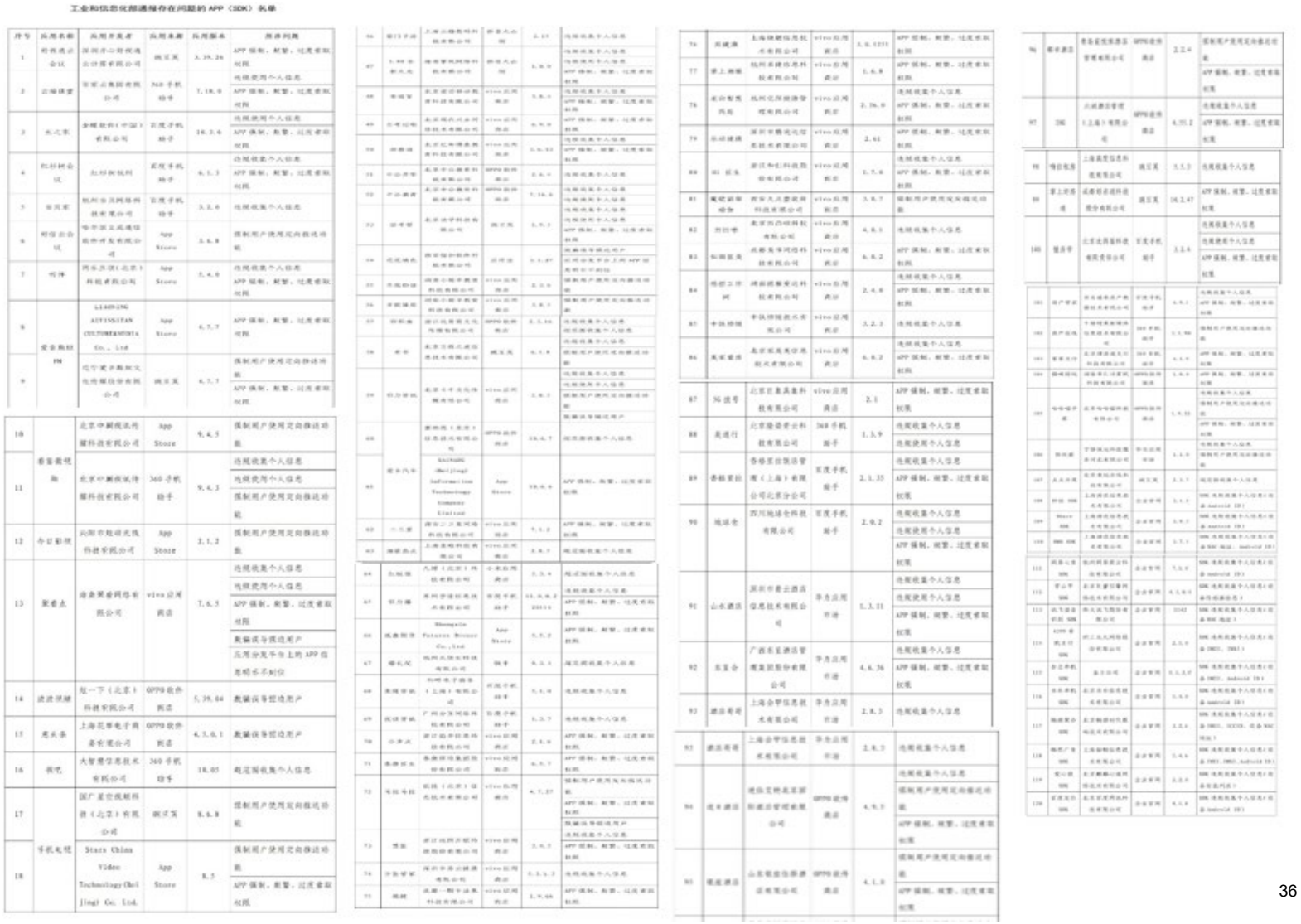
关于侵害用户权益行为的APP通报（2022年第1批，总第21批）

依据《个人信息保护法》《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，我部近期组织第三方检测机构对移动互联网应用程序(APP)进行检查，截至目前，尚有107款APP未完成整改。同时，检测过程中发现，13款内嵌第三方软件开发工具包（SDK）存在违规收集用户设备信息的行为（详见附件）。

上述APP及SDK应在2月25日前完成整改落实工作。逾期不整改的，我部将依法依规组织开展相关处置工作。

附件：工业和信息化部通报存在问题的APP(SDK)名单

工业和信息化部信息通信管理局
2022年2月18日



List of APPs penalized on the grounds of PIPL, CSL, etc.

关于侵害用户权益行为的APP通报（2022年第4批，总第24批）

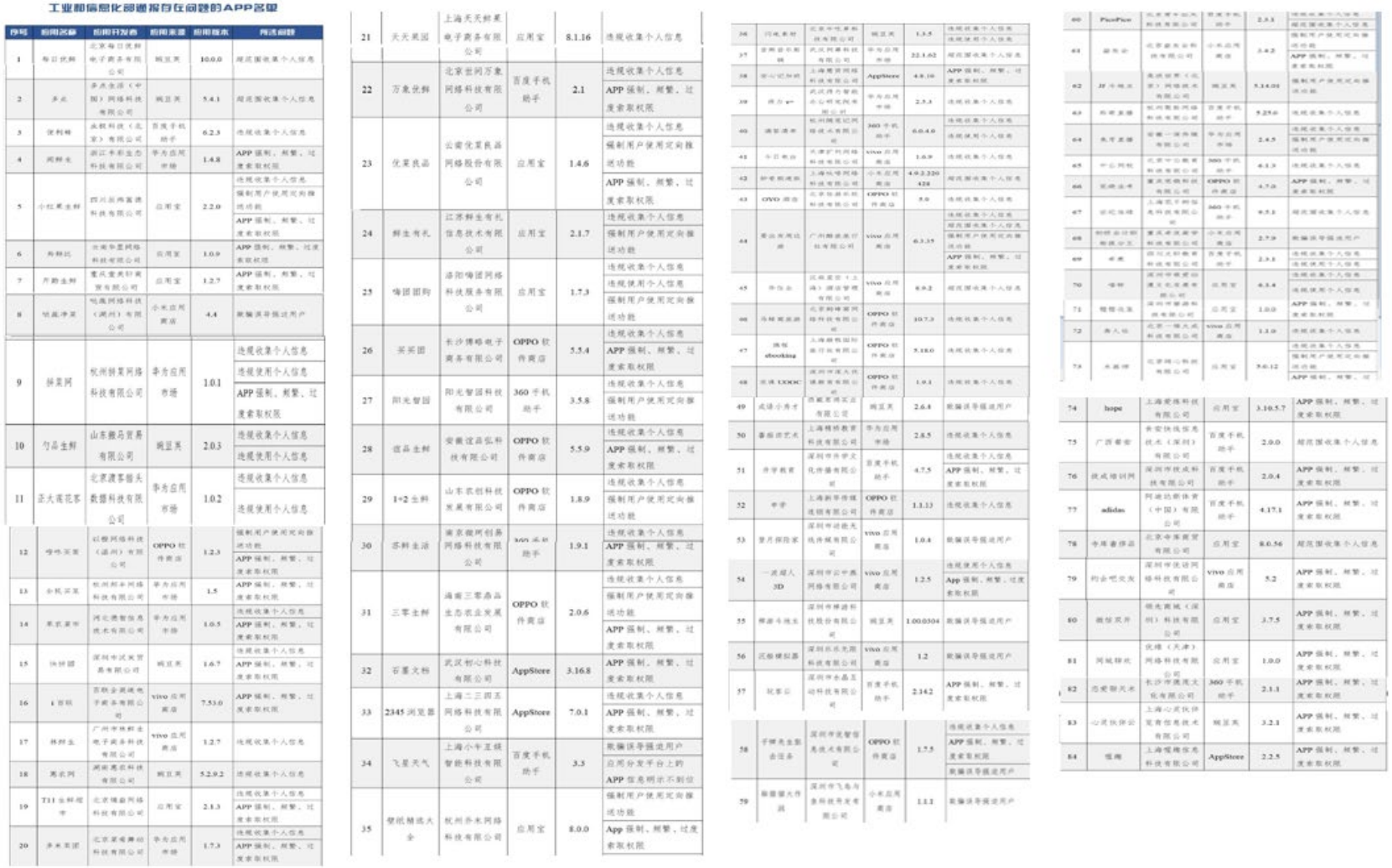
依据《个人信息保护法》《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，我部组织第三方检测机构对群众关注的生活服务类、日常工具类等移动互联网应用程序（APP）进行检查，对发现存在侵害用户权益行为的368款APP提出整改要求。截至目前，尚有84款APP未按要求完成整改（详见附件），现予以通报。

上述APP应在6月8日前完成整改落实工作。逾期不整改的，我部将依法依规组织开展相关处置工作。

附件：工业和信息化部通报存在问题的APP名单

工业和信息化部信息通信管理局

2022年5月31日


工业和信息化部通报存在问题的APP名单

Companies penalized for using facial recognition technology in contravention of PIPL

非法收集个人信息多家企业被罚

向行政机关送达诉前检察建议

本报讯 刘辉 曾永发 记者陈佳摄影报道：《个人信息保护法》已于本月开始施行，近期，赣州市检察院践行“我为群众办实事”、发挥检察公益诉讼职能，对部分商家安装人脸识别摄像头违规收集个人信息问题进行立案调查，并向相关行政机关发出诉前检察建议。截至目前，检察建议所涉问题已基本整改到位，主管行政机关依法对多家案涉企业处罚款共105万元。

商家非法收集个人信息

前段时间，赣州市检察院接到网友反映，赣州部分楼盘售楼部安装人脸识别摄像头侵犯公民个人肖像权。对此，该院立即组织人员进行线索摸排，发现情况确实存在。调查过程中，检察机关发现除房地产行业外，家装建材市场、汽车4S店等商家也存在安装人脸识别摄像头收集消费者个人信息的情况。

Criminal enforcement against violations under PIPL, etc. law

中国发布丨2021年打击侵犯公民个人信息犯罪十大典型案例公布

中国网1月10日讯（记者 张艳玲）记者从公安部获悉，2021年，全国公安机关深入推进“净网2021”专项行动，针对人民群众关注的个人信息保护问题，全力组织开展侦查打击工作，共破获侵犯公民个人信息案件9800余起，抓获犯罪嫌疑人1.7万余名，有力维护了网络空间秩序和人民群众合法权益。公安部日前公布了2021年侵犯公民个人信息犯罪十大典型案例。

一、江苏公安机关破获何某非法获取公民个人信息案。江苏公安网安部门侦查查明，犯罪嫌疑人何某利用为相关单位、企业建设信息系统之机，非法获取医疗、出行、快递等公民个人信息数十亿条，搭建对外提供非法查询服务的数据库，通过暗网发布广告招揽客户，出售谋取不法利益。

二、湖北公安机关破获徐某等人利用外挂程序非法获取公民个人信息案。湖北公安网安部门侦查查明，武汉某公司工作人员徐某等人，利用李某编写的多款外挂程序，通过系统接口漏洞，窃取酒店、燃气、医疗健康等33个网站后台公民个人信息3000余万条用于债务催收等。

三、安徽公安机关破获吴某等人非法获取老年人个人信息推销虚假保健品案。安徽公安网安部门侦查查明，犯罪嫌疑人吴某成立多家健康咨询公司，通过网上购买、交换有保健品购买记录的老年人信息200余万条，通过制定话术、夸大效果推销虚假保健品，骗取6万余名老年人1500余万元。

四、江苏公安机关破获关某等人非法获取公民个人信息案。江苏公安网安部门侦查查明，犯罪嫌疑人关某利用多个空壳公司与多家电信运营商签订合同，非法获取电信用户手机上网标签数据2亿余条，按照地域、行业等分类后，向下游精准营销人员和电信网络诈骗犯罪人员贩卖牟利。

五、福建公安机关破获谢某等人利用木马窃取网民购物信息案。福建公安网安部门侦查查明，犯罪嫌疑人谢某诱骗某电商平台店铺客服点击木马链接，窃取200余家店铺的买家个人信息1000余万条，向林某等人层层贩卖，最终流向电信网络诈骗团伙。

六、辽宁公安机关破获石某等人非法获取公民信息注册游戏账号并向未成年人出售案。辽宁公安网安部门侦查查明，山东某网络科技公司从网上购买公民信息，在辽宁阜新石某团伙的技术支撑下，突破游戏公司验证机制，非法注册实名网络游戏账号1.8万余个，向未成年人出售，非法牟利170余万元。

七、广东公安机关破获某公司非法获取公民个人信息实施诈骗案。广东公安网安部门侦查查明，珠海某艺术品策划公司从某APP维护人员汪某处购买APP在运营过程中获取的古董持有人员个人信息200万余条，以协助拍卖古董为名，骗取客户服务费、托管费，非法牟利1.9亿余元。该公司员工邝某、黄某为谋取私利，将公司非法获取的个人信息向其他电信网络诈骗团伙贩卖。

八、江苏公安机关破获某公司非法获取公民个人信息案。江苏公安网安部门侦查查明，某公司非法搭建5300余个虚假网站，冒用其他公司资质在某自媒体平台发布免费领取男科用药、白酒、保健品等虚假信息，引流至其所建虚假网站，骗取网民的姓名、手机号、收货地址等公民个人信息110余万条并贩卖牟利。

九、浙江公安机关破获李某等人非法获取公民快递信息案。浙江公安网安部门侦查查明，犯罪嫌疑人李某指使团伙成员应聘多家快递公司临聘人员，利用整理快递包裹之机，偷拍快递面单2万余张，汇总整理后在网上贩卖。

十、江苏公安机关破获张某等人非法获取公民个人信息案。江苏公安网安部门侦查查明，犯罪嫌疑人张某搭建服务器制作远程控制软件，出售给他人安装在受害人手机上，非法获取受害人手机的位置、通话记录等，涉及手机1.1万余台。

公安机关网安部门将会同有关部门，认真贯彻落实《刑法》和《个人信息保护法》《数据安全法》等法律法规，完善打击危害公民个人信息和数据安全违法犯罪长效机制，坚持打击和防范并重，做好源头防控，持续保持严打高压态势，不断提升人民群众的安全感。公安机关提醒广大群众，个人信息关系到每个人的合法权益和生命财产安全，保护自己和他人的个人信息安全人人有责。一旦发现个人信息被泄露，要及时向公安机关报案。实施侵犯公民个人信息违法犯罪，必将受到法律严惩。

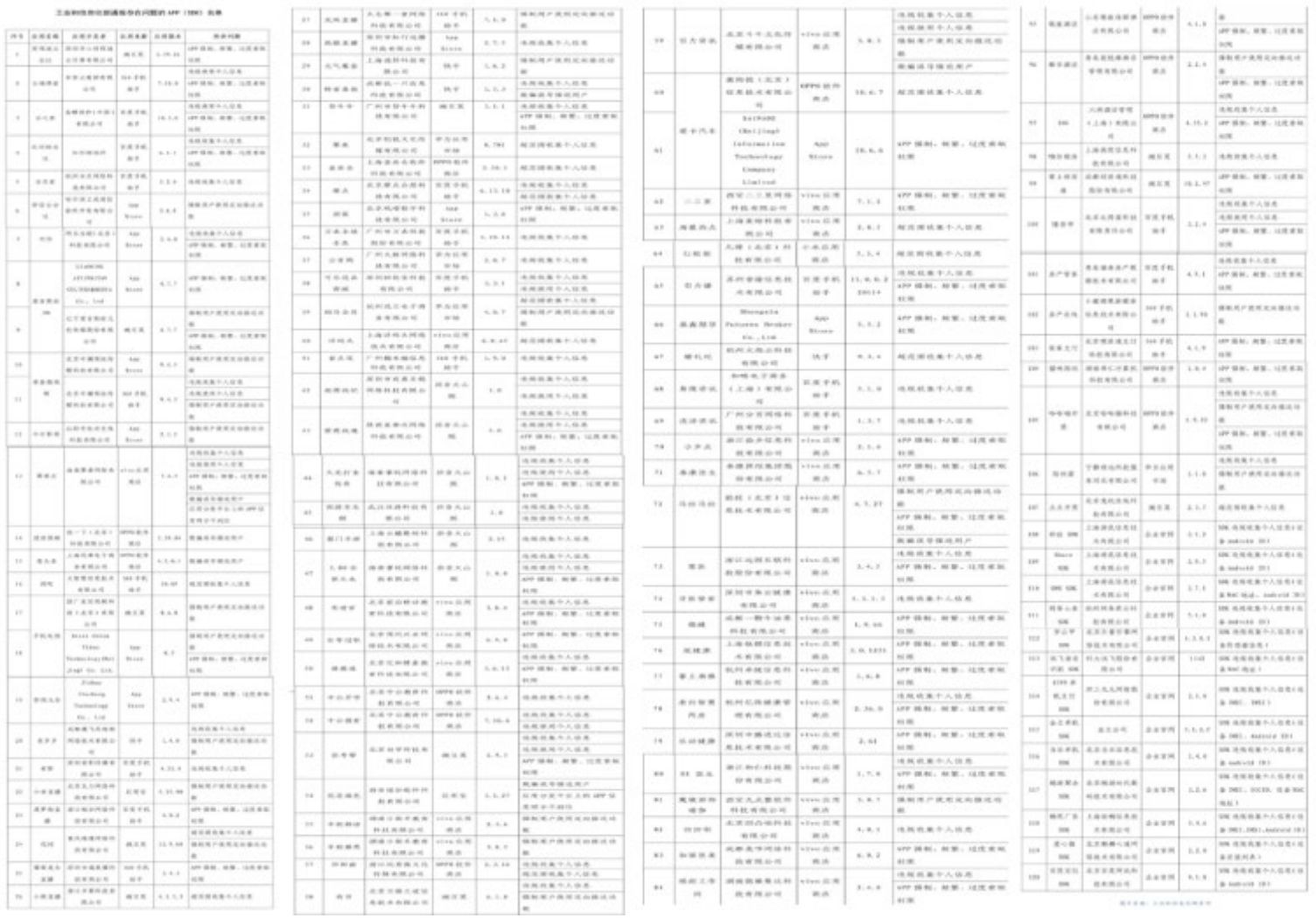
List of APPs penalized on the grounds of PIPL, CSL, etc.

工信部公布今年首批侵害用户权益APP 洋码头、中公教育等在列

2022年02月19日09:55 | 来源：人民网小字号

人民网北京2月19日电（申佳平）据工业和信息化部官网消息，依据《个人信息保护法》《网络安全法》《电信条例》《电信和互联网用户个人信息保护规定》等法律法规，工业和信息化部近期组织第三方检测机构对移动互联网应用程序(APP)进行检查，截至目前，尚有107款APP未完成整改，洋码头、中公教育等APP在列。

同时，检测过程中发现，13款内嵌第三方软件开发工具包（SDK）存在违规收集用户设备信息的行为。工业和信息化部要求相关APP及SDK应在2月25日前完成整改落实工作。逾期不整改的，将依法依规组织开展相关处置工作。



Ministry of Public Security: > 9,800 personal data infringement cases were investigated & ~ 17,000 criminal suspects arrested in 2021 for violating the PIPL and Data Security Law (7 May 2021)

公安部：2021年共侦办侵犯公民个人信息案9800余起1.7万名嫌疑人被抓

海报新闻记者 刘璐 北京报道

5月7日，公安部召开新闻发布会，公安部新闻发言人李国忠表示，一年来，维护网络空间安全和网上秩序成效显著。聚焦网上突出违法犯罪和网络乱象，连续组织“净网”专项行动，切实保障数字经济健康发展，维护人民群众合法权益。

公安部：2021年共侦办侵犯公民个人信息案9800余起1.7万名嫌疑人被抓

5月7日，公安部召开新闻发布会。

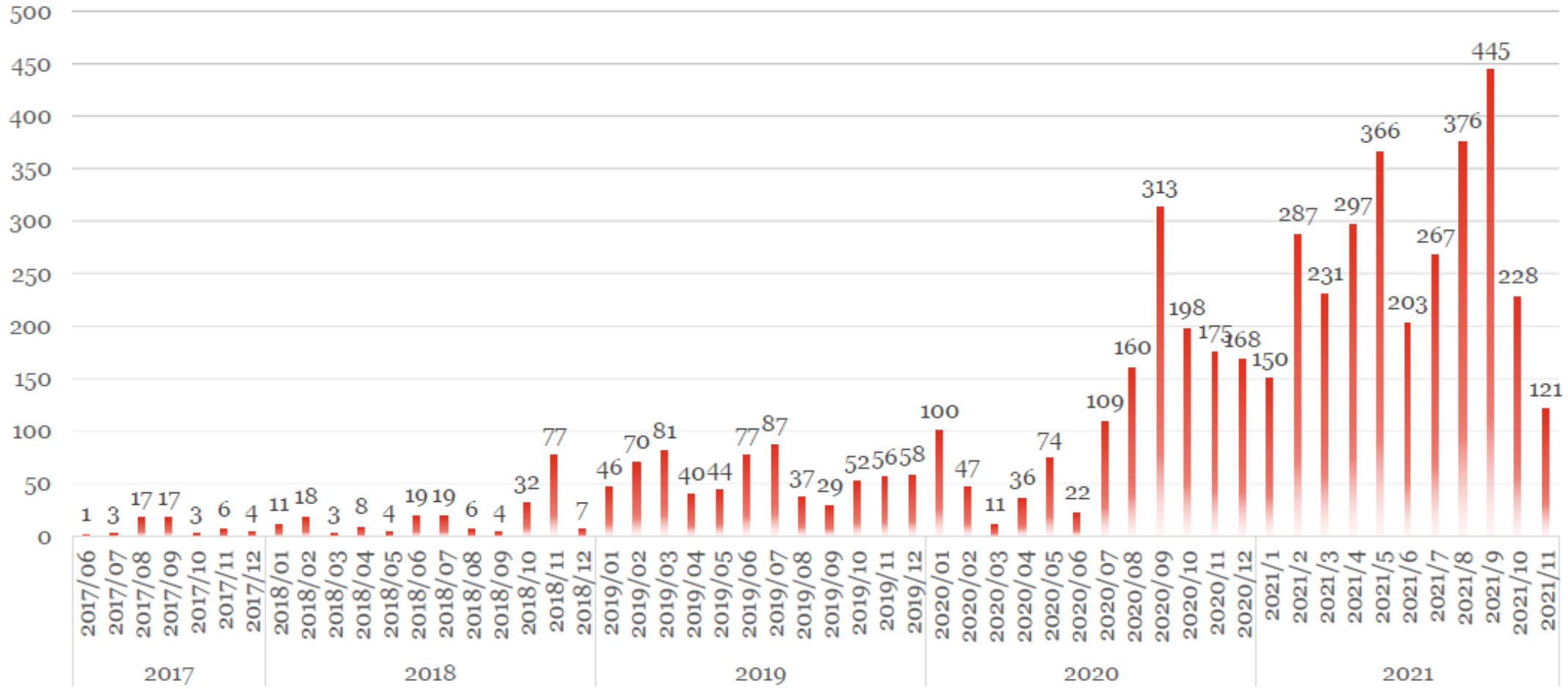
“净网2021”专项行动期间，共侦办案件6.2万起，抓获犯罪嫌疑人10.3万名，同比分别上升10.7%、28.7%。

深入贯彻《数据安全法》《个人信息保护法》，共侦办侵犯公民个人信息案件9800余起，抓获犯罪嫌疑人1.7万名。

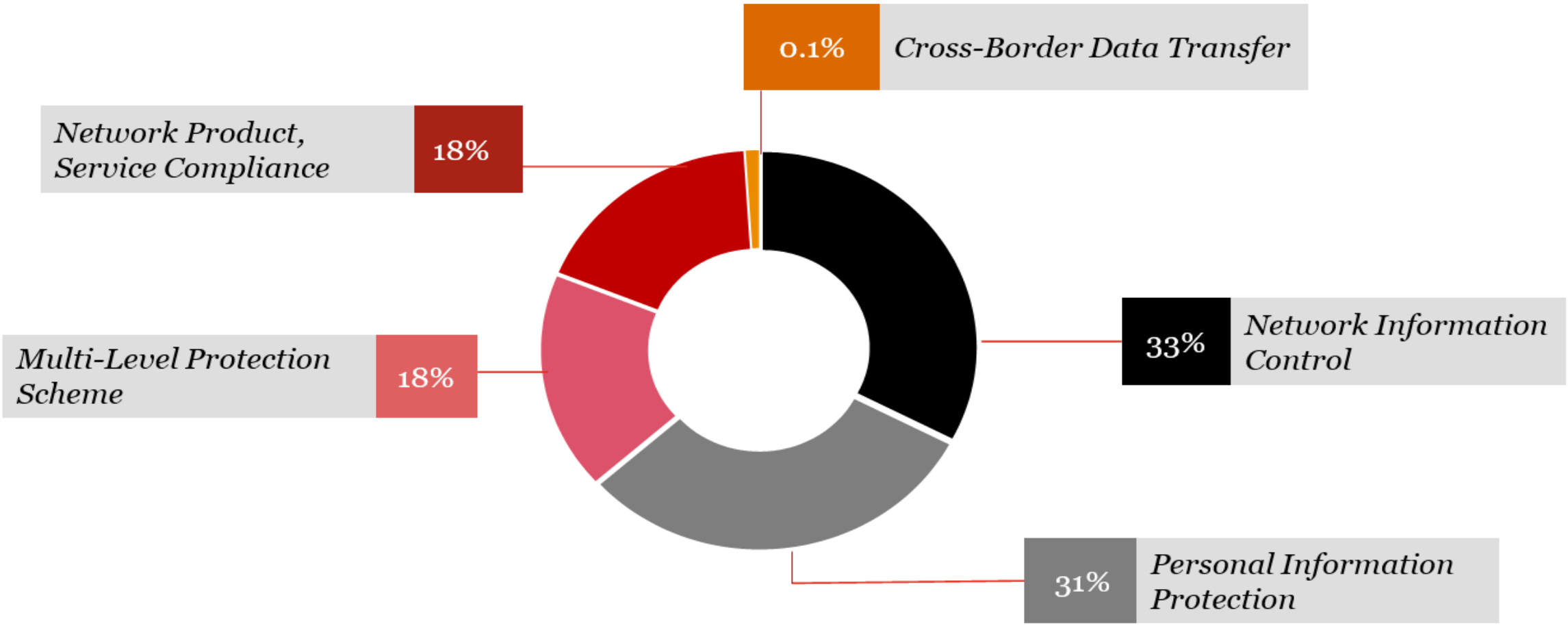
依法严厉惩治黑客攻击犯罪，共抓获实施黑客攻击活动及为其提供工具、洗钱等服务的人员3309名，铲除制售木马病毒、开发攻击软件平台团伙341个。

开展行政执法检查48117家（次），行政处罚互联网企业、单位2.7万家（次）；会同有关部门依法查处涉赌、涉淫秽信息突出的网络游戏134款；深入开展青少年网络环境专项整治，对1.3万个网络平台开展执法检查，行政处罚761家，限期整改2545家，清理相关违法有害信息约102.3万条。

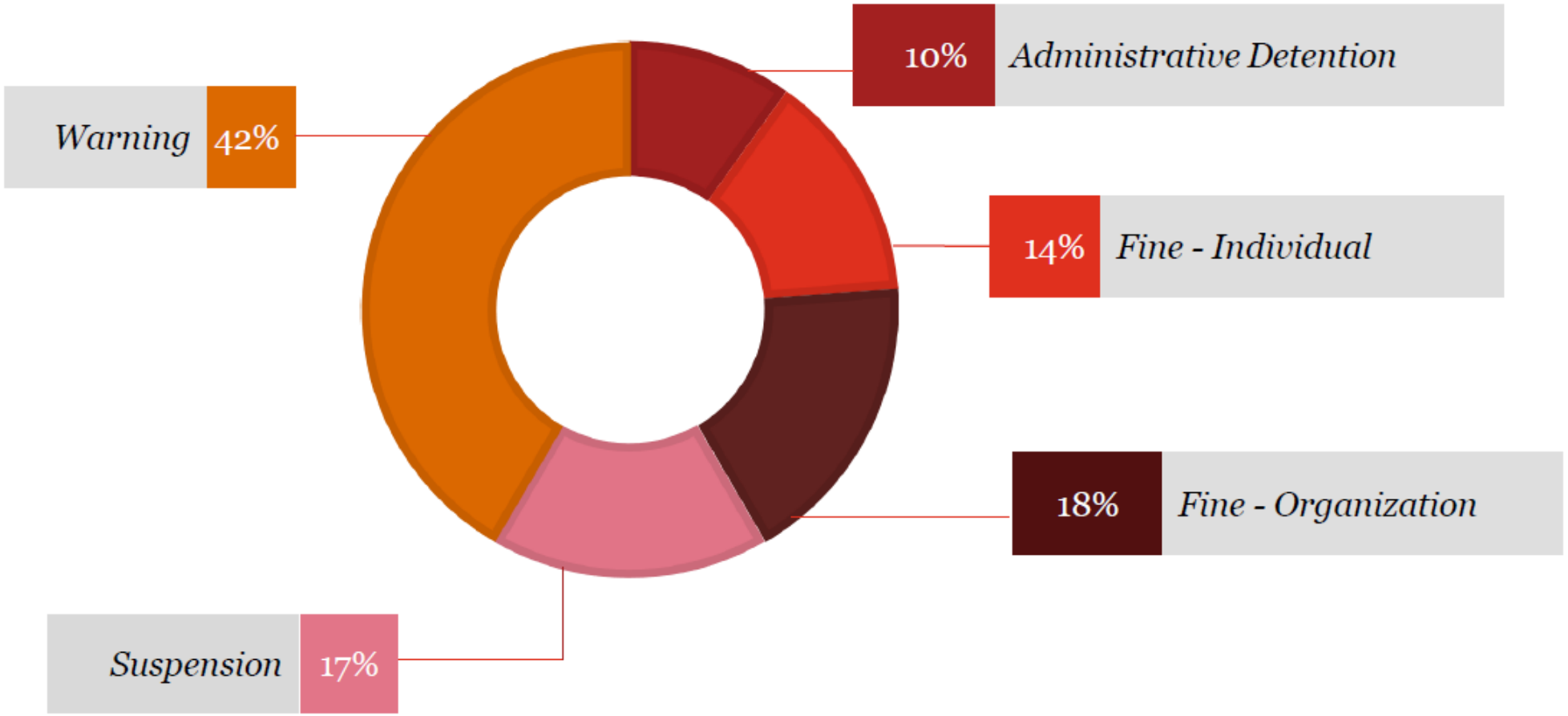
Enforcement – Time Distribution



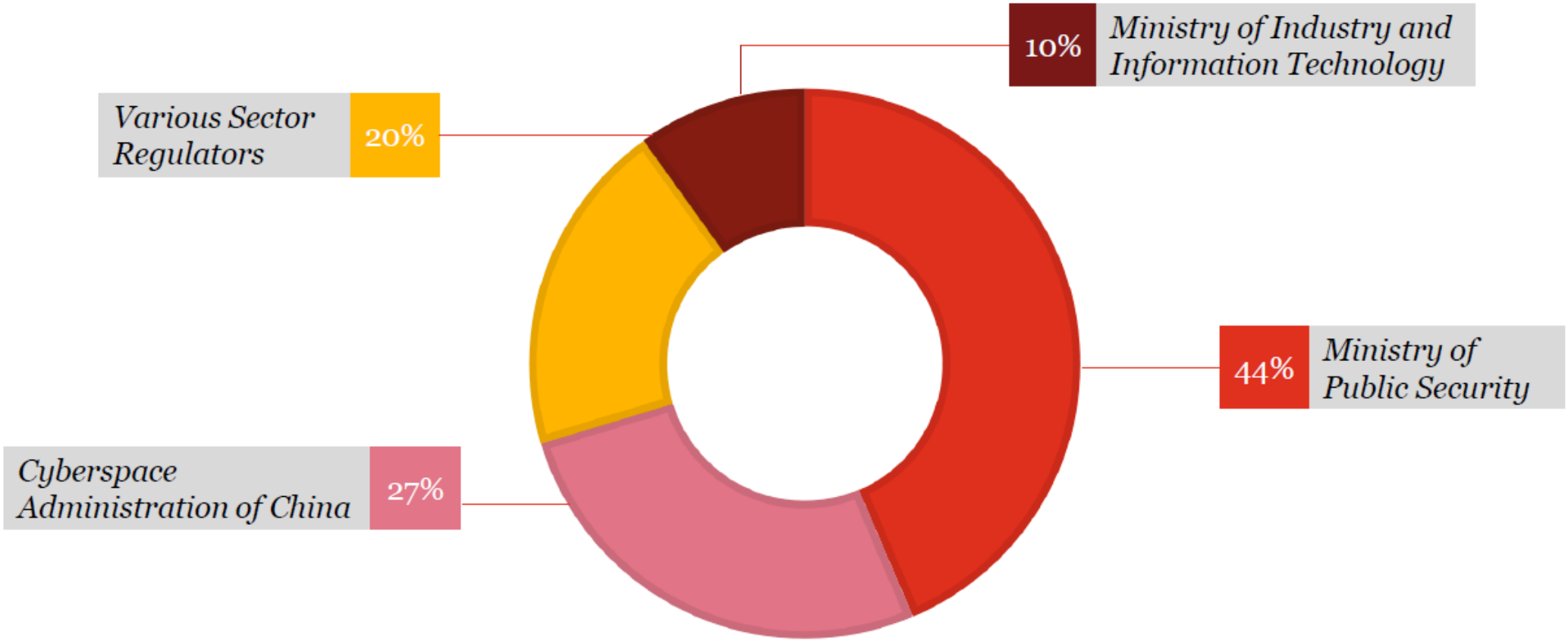
Enforcement – Areas of Non-compliance



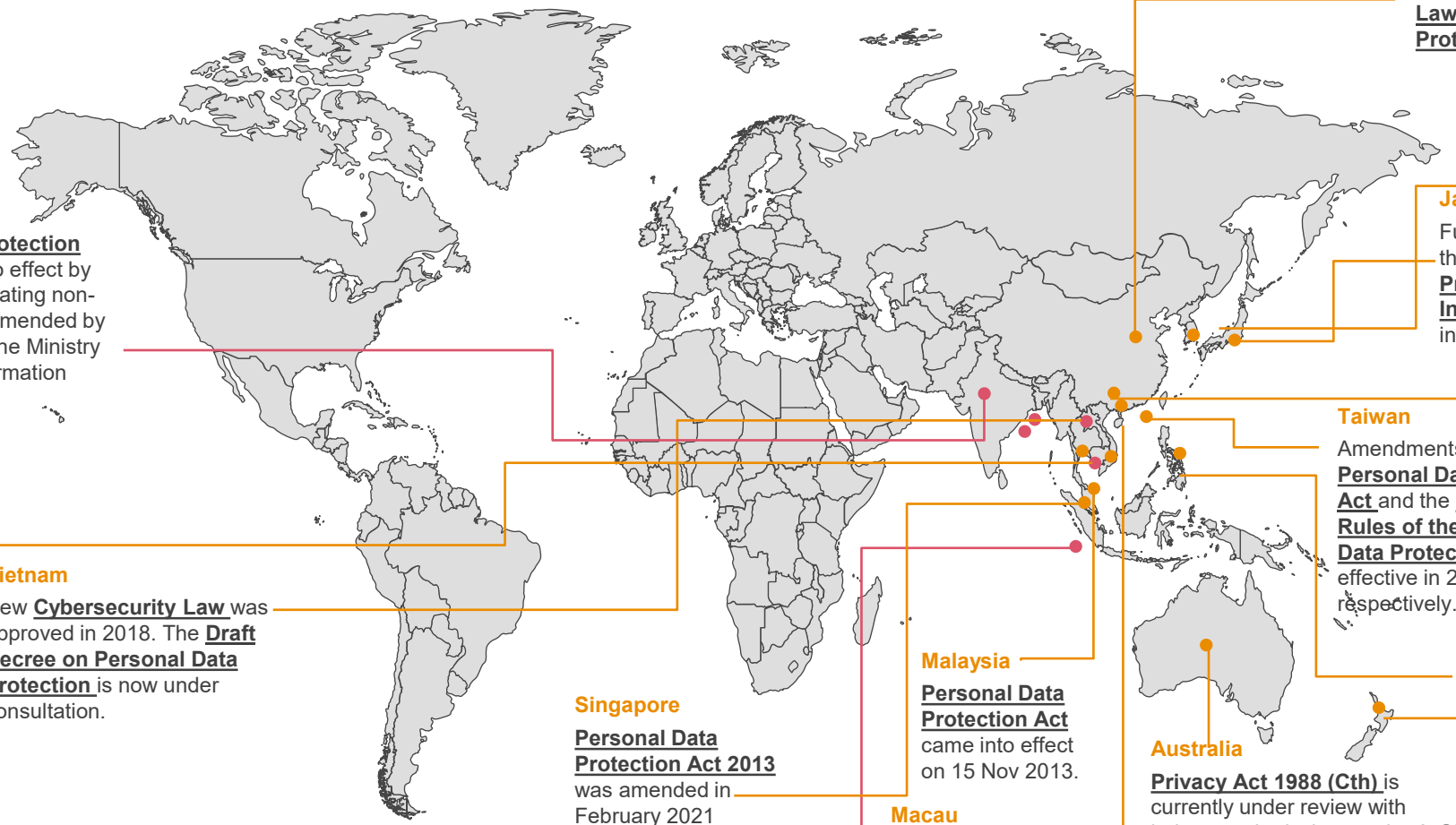
Enforcement – Penalties



Enforcement – Regulators



Asia Pacific Cyber & Data Developments 亚太网络安全及个人数据发展



China

Cybersecurity Law effective 2017. **Data Security Law** effective Sept 1 and **Personal Information Protection Law** effective Nov 1, 2021.

India

The **Personal Data Protection Bill 2019** will come into effect by the end of 2021. Regulating non-personal data is recommended by the committee under The Ministry of Electronics and Information Technology.

Thailand

After a Covid-19 delay, the **Personal Data Protection Act** finally became effective on 1 June 2021.

Vietnam

New **Cybersecurity Law** was approved in 2018. The **Draft Decree on Personal Data Protection** is now under consultation.

Singapore

Personal Data Protection Act 2013 was amended in February 2021

Indonesia

Laws on Electronic Information and Transactions restrict the electronic use of private data without the data subject's consent were amended in 2016.

Malaysia

Personal Data Protection Act came into effect on 15 Nov 2013.

Macau

The Personal Data Protection Law no.8/2005 came into force on 4 August 2005. **Macau Cybersecurity Law** effective 21 Dec 2019.

Australia

Privacy Act 1988 (Cth) is currently under review with industry submissions to the A-G's discussion paper due on 10 January 2022. **Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021,** introducing a binding Online Privacy code for social media services, data brokers and other large online platforms.

Japan

Further amendments to the **Act on the Protection of Personal Information** will come into force in 2022.

South Korea

Amendments to **Personal Information Protection Act** and the **Act on Promotion of Information and Communications Network Utilization and Information Protection** became effective in 2020.

Taiwan

Amendments to the **Personal Data Protection Act** and the **Enforcement Rules of the Personal Data Protection Act** were effective in 2015 and 2016 respectively.

Hong Kong

Changes regarding doxing have come into effect. HK Government announced law reform plan for HK data privacy law.

Philippines

Data Privacy Act came into effect in September 2012.

New Zealand

Amendments to the **Privacy Act**, alongside other codes that modify the operation of the Act were issued in 2020.

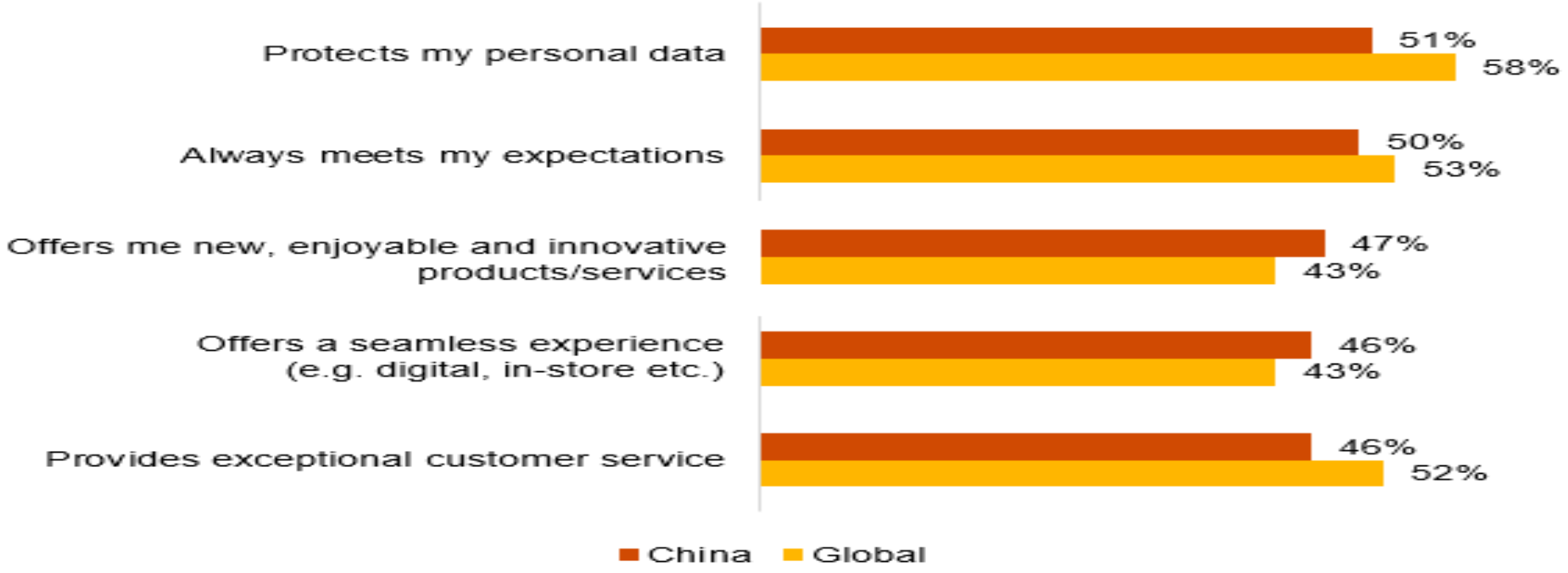
Data privacy protection laws / legislations in place

No overall or limited data privacy protection laws / legislations currently in place

Protection of personal data remains top factor for brand trust

- ✓ 51% of Chinese consumers (7 percentage points lower than Global) saying protection of personal data impacts how much they trust a brand

Q. Thinking about a brand that you regularly buy products/services from, to what extent do the following impact how much you trust the brand? The brand… (only showing 'To a great extent' answers)



Source: PwC's 2022 Global Consumer Insights Survey

Protection of personal data remains top factor for brand trust (cont'd)

- ✓ 63% of Chinese consumers said they are open to sharing their personal data only if it won't be shared or sold to other companies or third-party providers
- ✓ 60% said they will only do so where there is a clear data security policy

Q. Thinking about your consumer data, to what extent do you disagree or agree with the following statements in relation to sharing it with organisations? (Only showing 'Agree' responses)

Source: PwC's 2022 Global Consumer Insights Survey

Questions and Answers

Thank you

www.pwc.com
www.tiangandpartners.com

© 2022 PricewaterhouseCoopers Limited. All rights reserved. Not for further distribution without the permission of PwC. PwC refers to the Hong Kong member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2022 Tiang & Partners. All rights reserved. Tiang & Partners is an independent Hong Kong law firm.