CAICT 中国信通院

智能终端产业
个人信息保护白皮书

（2018 年）

中国泰尔实验室
中国互联网协会
电信终端产业协会

2018年11月

版权声明

前 言

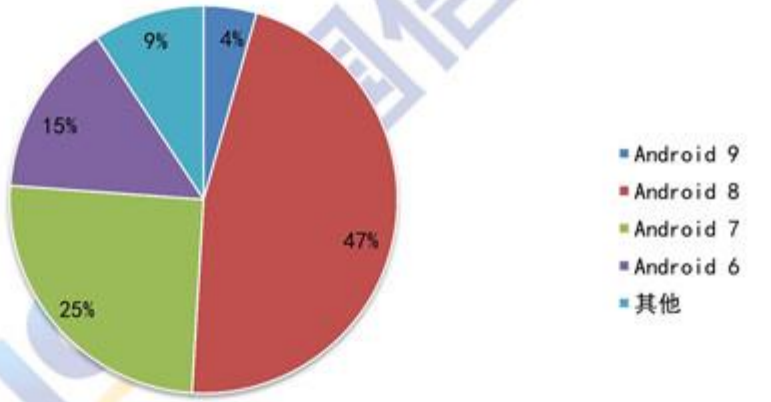
当前，世界正处于新一轮科技革命和产业革命的变革浪潮中，以智能终端为代表的互联网产业已成为“互联网+”的基础设施，是推动经济社会变革的重要力量。智能终端、应用分发平台、应用软件的迅猛发展为用户带来了前所未有的丰富体验。在智能终端上，可以通过应用分发平台下载社交、购物、支付、出行、娱乐等各类应用软件，随时随地享受互联网时代的便利。随着产业的蓬勃发展，终端产业未来会进一步走向信息化、智能化。

然而，随着技术日新月异的发展，智能终端产业的个人信息保护问题日益凸显，信息泄漏、信息过度收集使用、权限滥用等问题严重威胁了广大人民群众的切身利益。为保障智能终端产业健康发展，维护用户合法权益，中国泰尔实验室、互联网协会、电信终端产业协会联合制定与发布本白皮书。本白皮书着眼于智能终端产业新的发展阶段，阐述了个人信息保护现状和面临的挑战，基于业界最佳实践，在终端设备、分发平台、应用开发等方面提出个人信息保护建议，并倡议产业界落实企业主体责任，加强行业自律，强化产业协作体系，共同构筑智能终端产业个人信息保护良好生态。

目 录

一、智能终端产业现状

据中国信息通信研究院发布的《2018 年 9 月国内手机市场运行分析报告》，2018 年 1 月到 9 月，国内智能终端出货量为 2.87 亿部，其中 Android 操作系统占比达到 89.8%，iOS 操作系统占比为 10.1%，其他系统为 0.1%。Android 操作系统具备开源、开放、灵活的特性，当前占据了智能终端市场的主导地位。随着用户权益保护意识的觉醒，装载 Android 操作系统的智能终端已成为个人信息保护工作的焦点。



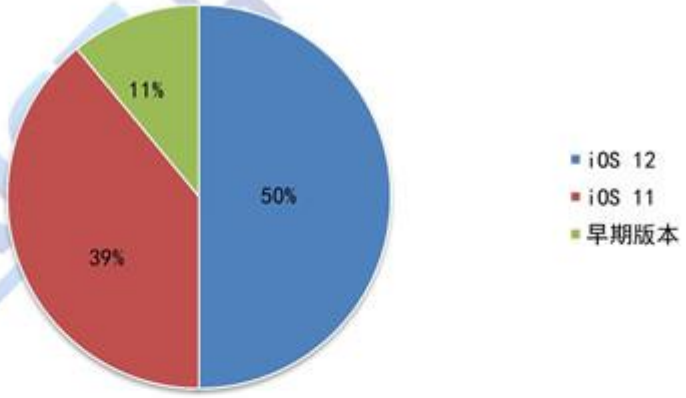
数据来源：中国泰尔实验室

图 1 2018 年进网终端 Android 系统版本比例

Android 系统碎片化问题严重。据统计，在 2018 年进网终端中，Android 9.0 占比 4.42%；Android 8.0 占比 46.54%；Android 7.0 占比 25.18%；上市三年多的 Android 6.0 系统，占比 14.58%；Android 5.0 及更早之前的版本占比 9.28%。相对于旧版本，新版本增加了更多的

个人信息保护机制。严重的系统碎片化问题，使得较多应用利用 Android 操作系统向下兼容的特性，采用较低等级目标 API 版本，规避高版本操作系统安全和保护机制的约束。

iOS 系统版本分布相对集中。根据苹果公司官网数据，截至 2018 年 10 月 10 日，全球活跃设备中有 50%使用 1 个月前发布的 iOS 12 新版本，约 90%的用户使用一年内发布的 iOS 版本。相对于 Android，iOS 操作系统具有封闭的特性，核心代码不开放，操作系统统一更新，新版本普及速率较快，版本分布比较集中，碎片化现象不严重。同时，具有唯一的官方应用市场（App Store）下载渠道，应用上架规则统一，可在源头加强应用敏感权限使用和信息收集使用的审核，对营造的 iOS 产业生态具有较强的管控能力。



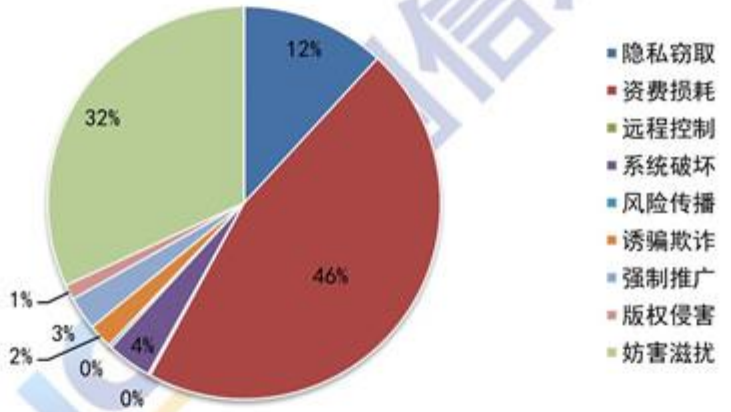
数据来源：苹果公司官网，2018 年 10 月 10 日

图 2 活跃设备 iOS 系统版本比例

应用个人信息保护问题突出。用户可从商店、网页、论坛等第三方分发渠道下载应用。装载社交、购物、支付、出行、娱乐等各类应

用的终端设备，已经成为用户社交和生活的主要载体。终端所装应用引发的信息泄露等问题是消费者关注的焦点。在应用使用过程中，用户让渡部分信息获取生活便利已成为普遍现象，大量应用越界获取及滥用用户信息，侵犯用户合法权益，造成用户财产损失。

敏感信息窃取比例11.86%。在2017年10月-2018年10月所检测的2722万余款应用中，存在资费损耗、妨害滋扰、隐私窃取等侵犯用户权益的应用299万个，其中窃取敏感信息的应用比例为11.86%。

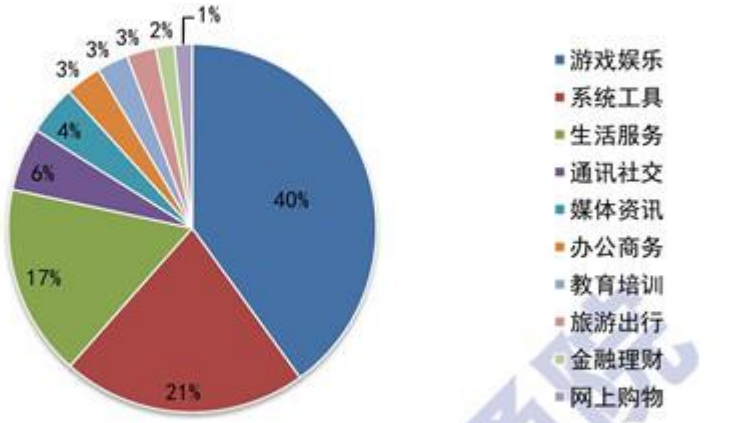


数据来源：武汉安天信息技术有限公司

图3 用户个人信息保护不良行为类别

游戏娱乐类应用风险最高。从高风险和违规应用分布来看，游戏娱乐类应用占比最高，达40.05%。游戏依托其应用特性，多款应用存在窃取用户信息、强行捆绑应用等问题。高风险和违规应用中系统工具类占比21.49%，其中手机桌面应用、ROOT工具应用等越界获取用户信息严重，甚至造成用户财产损失。生活服务类应用占比16.83%，该类应用与用户生活连结紧密，更容易被攻击者利用，窃取

用户信息，侵犯用户权益。



数据来源：武汉安天信息技术有限公司

图 4 高风险和违规应用行业分布

二、智能终端产业个人信息保护面临的挑战

随着大数据时代的到来，个人信息保护问题逐渐暴露。信息泄漏、信息过度收集使用、权限滥用等问题严重威胁了广大用户的切身利益。应用 API 等级低、一揽子授权、不授权就不给用等现象的存在，将用户推入隐私与便利的两难选择。智能终端产业用户个人信息保护工作面临严峻的挑战。

（一）用户信息过度收集难识别难举证

随着移动互联网的迅速发展，应用经历了“野蛮生长”的时代。为提供个性化服务，开展精准投放，应用收集使用了大量用户的个人信息，包括设备信息、位置信息、通讯录等敏感数据。应用在收集使用个人信息的过程中，存在以下现象：

应用在用户不知情的情况下，过度收集和使用个人信息。大量用户反映，个人信息在不知情的情况下被收集使用，搜索过的信息，说过的话，敏感的健康数据，以用户可感知的方式呈现。但信息是如何被收集，通过何种渠道共享传播，普通用户难识别，难举证。较多应用并未通过隐私政策或其他途径告知用户收集使用信息的目的、方式和范围，也未向用户提供明确的允许和拒绝的选择，这种累积性的权益侵害在日常生活中普遍存在，引发了用户的严重担忧。信息过度收集使用的乱象亟待解决。

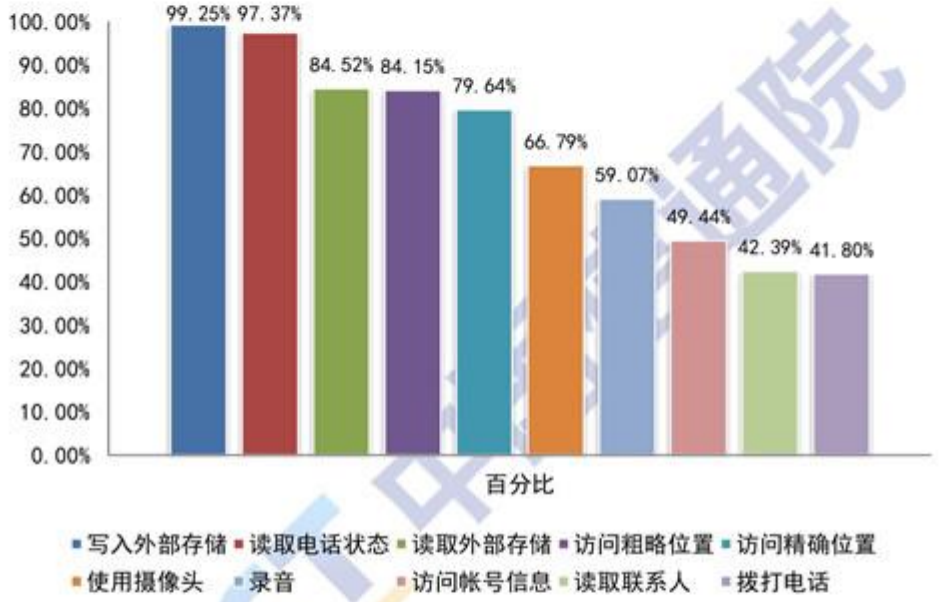
应用第三方SDK大量收集使用个人信息。应用通常会使用第三方SDK快速实现业务功能，而第三方SDK与应用在收集用户信息方面具有同样的能力。鉴于第三方SDK的不开源性，应用无法完全掌控第三方SDK的行为。部分应用不清楚SDK申请权限的目的，难以准确明示第三方SDK所收集使用的用户信息，通常只能通过协议约束第三方SDK收集使用用户信息的行为。某些第三方SDK同时被多家应用集成使用，收集的海量数据一旦泄露，可造成广泛的恶劣影响。

（二）权限申请过度易感知难判定

权限是指为保护用户的隐私，移动终端操作系统对于应用访问敏感用户数据或使用特定系统功能的限制。为满足用户可知可控要求，国内终端大都具备权限管理机制，权限申请在显著位置提示，并经用户同意后方可使用。但目前权限申请过度仍是普遍现象。

权限申请过度现象严重。根据对国内应用市场TOP 1000应用取样分析显示，Android应用普遍会申请电话、定位、摄像头和录音等

核心敏感权限，其中读取电话状态权限的比例 97.37%，申请位置权限的比例 84.15%，申请摄像头权限的比例 66.8%，申请录音权限的比例 59.1%，申请联系人权限的比例 42.4%。应用过度申请权限的问题普遍存在。申请超出应用实际业务功能和场景的权限，为应用过度收集用户个人信息打开了通道，极易造成用户信息泄漏。



数据来源：中国泰尔实验室

图 5 应用权限获取情况

权限过度申请滥用难规范难判定。如何判定应用权限过度申请和滥用，存在易感知难判定的问题。目前尚缺乏成熟的技术规范和判定手段，难以正确引导应用开发者遵循合法正当必要原则申请权限，是智能终端产业在个人信息保护工作中面临的巨大的挑战。

（三）低 API 等级应用规避安卓安全机制

应用与 Android 系统的交互依赖于框架 API，开发时要配置应用

的目标 API 等级以明确应用支持的 Android 目标系统版本。

低 API 等级应用风险高，升级难度大。Android 系统在应用运行时检查目标 API 等级设置，若系统版本低于或者等于应用的目标 API 等级，系统无需执行任何兼容性处理。若 Android 系统版本高于此项配置，系统会执行兼容性策略。低 API 等级应用运行在高版本的 Android 操作系统上，可绕过 Android 系统的信息保护机制。同时，Android 系统针对目标 API 等级 23 及以上的应用执行运行时权限机制，即业务功能运行时系统才会授予应用权限。目标 API 等级 23 以下的应用采用一揽子授权，存在不授权无法安装使用的问题。目前，国内应用达到目标 API 等级 26 及以上的比例大致为 10%，推动应用开发者及时适配高版本 Android 系统，加强移动智能终端预置与分发环节对应用高 API 等级的上架要求，是近期用户个人信息保护的重点工作。

（四）设备识别码防护意识不足

随着大数据产业的发展，收集智能终端唯一标识，如国际移动设备识别码（IMEI）、Wi-Fi MAC 地址、SIM 卡国际移动用户识别码（IMSI）和蓝牙地址等设备物理地址信息成为普遍现象。

用户普遍缺乏设备识别码防护意识。设备识别码与用户身份深度绑定。累积性的数据汇聚为用户的行踪轨迹，可用于分析特定用户的生活习惯和消费行为，形成个人画像，并在用户未知情的情况下用于精准营销、甚至精准诈骗等。然而普通用户缺乏设备识别码的防护意识，并未意识到设备识别码已成为重要的个人敏感信息。提升用户设

备识别码防护意识，加大设备识别码保护机制研究，落实设备识别码防护措施，既是个人信息保护工作的难点，也是重点。

设备识别码防护手段不足。部分终端设备使用了Wi-Fi MAC地址随机化机制，在未接入Wi-Fi热点时发送含有随机MAC地址的探索帧，避免真实MAC地址被恶意Wi-Fi热点非法收集，防止用户轨迹的泄露。但当终端设备实际接入Wi-Fi网络时，终端设备仍需切换真实的MAC地址进行网络通信，未能从根源上解决设备识别码被非法收集的问题。

（五）隐私与便利选择两难，产业协作能力不足

移动互联网在给我们工作生活带来便利的同时，频频出现用户个人信息泄漏、盗用等问题。

隐私换取便利是无奈之举。大量应用在安装使用时，申请通讯录、摄像头、短信、录音、位置等多项与其核心功能无关的权限，若用户拒绝某些权限的申请，应用则无法正常使用。这种行业内普遍存在的一揽子授权、不授权就不给用的现象，使得大部分用户别无选择，不得不拿个人隐私换取便利。应用这种权限滥用行为，已经成为用户个人信息泄露的主要途径。

产业协作能力不足。在用户权益保护共识广泛达成、公众个人敏感信息保护意识普遍提升的情况下，终端、应用、分发等产业链环节协作不足，权限管控、信息收集使用、设备识别码防护等方面行动不统一，未形成有效合力。建立对重点环节的有效管控，构筑上下游打

通、各方力量协同的个人信息保护协作体系，将成为现实需要和必然方向。

三、终端设备个人信息保护的分析和建议

随着互联网的迅猛发展，终端功能日益丰富，在给生活带来极大便利性的同时，也逐步成为绑定了大量个人信息的载体，带来安全威胁。终端设备应从权限可知可控，个人信息采集告知同意，设备识别码安全防护，生物特征数据保护，终端设备应用管控和基础保障等多个方面出发，建立全方位的个人信息保护体系，为个人敏感数据的机密性、完整性和可用性保驾护航。

（一）加大权限调用可知可控力度

应依据YD/T 2407-2013《移动智能终端安全能力技术要求》标准，终端设备应遵循行为与用户意愿一致的基本原则，设计完善的权限管控机制，提升用户可知可控的能力，避免用户个人信息泄露。

用户对终端设备权限调用应可知。终端设备应通过给用户提示的方式来防范安全威胁，给用户的提示可以是图标、文字或其他明显的方式。在操作执行期间，提示应足够引起用户注意，且提示信息易于理解。终端设备宜从应用和权限两个视角呈现调用情况，用户既可查看单个应用申请的全部权限及目的，也可查看申请某特定权限的全部应用。同时，建议终端设备提供相应机制，在一定时间内记录并统计应用调用行为情况，可供用户查看详细记录结果。

用户对终端设备上权限调用应可控。终端设备应通过让用户确认

的方式来防范安全威胁，用户应具有选择权，即用户能确认也能取消。Android 6.0（API 23 等级）及以上，在应用运行时向其授予权限。终端设备应提供权限管控机制，对所安装的第三方应用的敏感权限进行分项控制，可提供允许、询问和禁止三种状态以便用户选择。终端设备在应用使用摄像头、录音、定位和电话等核心敏感权限时，应实时提供显性提示告知用户。手机号码、设备识别码（IMEI、Wi-Fi MAC 地址等）、读取短信、写/删短信、读取联系人、写/删联系人、后台截屏、上网记录（历史、书签）等敏感权限，应在相关业务功能运行时获取用户确认授权。终端设备未经用户许可不得默认授权。应用调用移动数据、WLAN、NFC 和蓝牙等功能开关时，应征得用户同意。终端设备宜提供应用自启动权限管理功能，用户可设置应用能否被系统或第三方应用启动。

（二）落实信息收集使用告知同意

终端设备在收集和使用个人信息时，用户应具有知情权与选择权。终端应详细告知所收集用户个人信息的内容、目的、方式和范围，仅当用户同意后方可收集。

在个人信息收集前告知用户。在企业网站、公众号等渠道明示终端及预置软件的相关信息，为用户选择终端产品提供便利的查询方式。用户首次使用时，终端设备应在开机向导的隐私政策、用户协议中，展现信息收集使用的内容，明确告知此设备将收集的详细信息。在首次使用功能或服务前、撤回授权后重新使用前，分项告知用户功

能或服务收集个人信息详情。在使用终端功能或服务过程中，需收集个人敏感信息时，应在每次收集前进行告知。当收集信息的内容、使用目的、收集方式与频率、存放地域与期限、保护方式、信息共享和个人信息控制权等发生变更时，应重新告知用户。

告知方式应易于用户感知。终端告知方式，应根据收集的信息类型、功能服务类别、终端设备形态等因素综合考量。可在通用隐私政策基础上，根据功能和服务的不同，制定独立的隐私政策。在终端界面中，应增加可供用户随时查看的隐私政策或用户协议入口。在个人敏感信息收集时，应通过询问、弹窗等二次增强的告知方式，将收集的个人敏感信息告知用户，并由用户选择同意或拒绝。可在终端告知方式上开展创新，如动画、短片等告知形式。

告知内容应足够清晰且易于理解。终端告知内容应准确、清晰、易懂，符合通用的语言习惯，避免歧义，不得诱导用户。告知内容应包含收集使用信息的内容、目的、方式、范围、频次、保护措施以及公开、转移、共享等相关信息。终端应明示用户对个人信息所拥有的各项权利，如拒绝权、访问权、更正权撤销同意权等。

（三）提高设备识别码防护能力

随着设备识别码敏感性的提升，用户高度关注设备识别码被收集滥用的情况。终端设备厂商应加强设备识别码的防护，提升设备识别码防护能力，避免在用户不知情的情况下，与用户身份绑定的物理设备信息被随意收集使用。

设备识别码匿名化。在终端设备的使用过程中，使用匿名化的设

备识别码机制，降低因设备识别码泄露用户位置记录、消费习惯等信息的风险。例如在连接 Wi-Fi 热点的过程中，终端设备使用随机化的 MAC 地址搜索 Wi-Fi 热点，可保护真实的 MAC 地址。此外应加快设备识别码匿名化方案的研究，提出切实可行的设备识别码匿名化框架，如研制真伪设备识别码映射系统、提出 Wi-Fi 协议识别码匿名化机制等。

提供设备识别码替代机制。终端设备应尽量避免使用设备识别码作为终端唯一标识符，应提供替代机制。例如采用广告 ID 作为唯一标识符，使终端设备应用无法获取设备物理的识别码，用作精准营销、用户画像等。同时该广告 ID 可由用户重置，禁止将设备识别码与广告 ID 链接，杜绝长期跟踪用户的行为。

严格限制获取设备识别码。终端设备应禁止设备直接获取所有的设备识别码，同时应对设备识别码的访问设置严格权限管控机制，如第三方应用对设备识别码的收集与使用应对用户详细提示与确认，并在用户同意后进行。

（四）重点加强生物特征数据保护

支付业务中的生物特征数据直接关系到用户的切身利益，用户的支付口令、生物识别信息等必须得到有效的安全防护。终端设备厂商应健全生物特征数据保护架构，采用生物特征数据加密存储、支付环境隔离防护等措施，保障用户切身权益。

生物特征数据应进行加密存储。为保障用户支付口令、密钥、证

书、指纹模版和人脸模版等个人敏感数据的安全性，建议使用具备安全存储功能的安全单元芯片（SE）、可信执行环境（TEE）等方案，存储加密后的个人敏感数据，加密的密钥应采用多密钥衍生的方式，保证终端设备一机一密。终端设备应遵循生物特征数据本地存储的原则，未经用户许可，严禁上传云端。

支付环境应采用隔离防护措施。支付环境应采用软硬件隔离技术，使用安全单元芯片（SE）、可信执行环境（TEE）等方案，将支付应用与其它应用进行隔离，确保在支付全生命周期中个人敏感数据不被非法窃取。

（五）完善应用管控保障机制

终端设备厂商应该构建完善的应用管控保障机制，提供应用签名、运行时内存保护、恶意网址检测、流量监控等措施，全方位保护用户数据。

使用应用签名。使用应用签名保证应用的完整性和来源的合法性，系统在安装应用时，通过对签名进行验证，检查应用是否被篡改。

运行时内存保护。通过地址空间布局随机化（ASLR）及数据执行保护技术（DEP），增加内存漏洞攻击的难度，降低个人敏感数据被窃取的风险。

提供恶意网址检测功能。针对短信、浏览器和即时通讯等应用中未知来源的链接，提供恶意网址检测功能。

监控流量使用情况。监控应用数据流量使用，将应用流量情况展示给用户，同时提供Wi-Fi和蜂窝移动网络的控制选项，防止恶意应

用后台上传个人敏感数据。

（六）加强基础保障能力建设

终端设备应提供基础安全能力和信任凭证，保障个人信息的机密性、完整性和可用性。

具备安全启动机制。终端设备应采用验证数字签名等安全启动机制，确保系统代码的可靠性和完整性，防止恶意代码的加载运行。

实施强制访问控制。使用 SELinux 对所有的进程、文件和操作等实施强制访问控制，阻止进程读写受保护数据和绕过内核的安全机制。

内核地址空间布局随机化（KASLR）。采用地址随机化技术，使内存地址空间随机化，防止攻击代码对内存中的地址进行硬编码，提升系统内核的安全性。

定期进行系统安全更新。系统升级可及时修复存在的漏洞。系统镜像更新时，应对升级包进行签名校验，并在用户同意后进行系统更新。

具备系统版本防回退手段。相比旧系统版本，新系统版本修补了部分已知漏洞，在安全机制、个人信息保护能力上有所提升，大幅降低了个人敏感数据泄露的风险。终端设备可通过版本校验等方式，防止系统回退到旧版本。

建立漏洞响应机制。终端厂商应建立健全漏洞响应机制，持续加固系统，保障系统安全；并提供反馈渠道，及时响应官方发布的漏洞

信息。定期更新安全补丁，提示用户进行安全更新，以便快速修复漏洞。

四、应用开发个人信息保护的分析与建议

开发者对应用权限申请和个人信息的收集、使用负有主体责任，应在应用的需求分析、设计、开发、上架、运营、维护和更新的全生命周期中，高度重视用户个人信息保护工作，全面维护用户的合法权益。

（一）采用高 API 等级开发应用

Android 6.0 引入了运行时权限机制，打破了权限的一揽子授权模式，用户可在运行时进行应用权限授予，可更好的了解和控制权限。Android 8.0 增强了用户数据保护能力，提出了后台位置限制、后台行为限制和广播限制等要求，对用户数据保护有积极的作用。Android 9.0 新增了多种数据加密机制，引入了对安全硬件、生物特征解锁的支持。

响应自律公约倡议，采用高等级 API 开发应用。开发者基于 Android 6.0（API 23）及以下版本开发应用时，系统默认授予应用申请的所有权限，若拒绝授予或者关闭某些权限，应用可能出现崩溃闪退等问题。基于此，电信终端产业协会发起《移动应用软件高 API 等级预置和分发服务自律公约》，倡议开发者使用 Android 8.0 (API 26) 及以上的版本进行应用开发，以保护用户权益。随着 Android 系统版本的更新，开发者应及时采用相对较高等级 API 开发应用。

（二）适配最新操作系统及外部代码库

智能操作系统会定期更新版本，并升级开发 SDK。以 Android 为例，谷歌每年会推出 Android 新版本，提升应用安全性并全面改善用户体验。

及时适配操作系统最新稳定版本。应用开发者进行软件开发时，应及时适配操作系统最新稳定版本，给用户带来较好的使用体验和较强的个人信息保护机制，避免旧版本的遗留问题影响应用使用，侵犯用户权益。对于集成第三方代码的移动应用，在采用新版本操作系统后，需适配相应第三方代码库，避免旧版本代码的兼容性引入新问题。

充分利用终端和操作系统新特性。在应用开发时，开发者应充分利用终端和操作系统新特性，例如可信执行环境（TEE），可信单元芯片（SE）和生物识别认证方式等。

（三）遵循合法正当必要原则申请权限

开发者在应用设计和开发时，重点关注应用权限的申请和使用，应遵循合法正当必要原则，将最小够用理念贯穿整个开发周期。

保证用户可知可控。开发者应以用户便于理解的方式，充分告知用户申请和使用权限的必要性，不应在用户不知情或者未获得用户许可的情况下，使用权限和收集用户数据。在描述相关权限、行为使用场景和使用目的时，开发者可使用图标、文字以及其他创新形式明确告知用户。在集成第三方 SDK 时，开发者应充分了解其申请权限的目的，对引发的后果承担相应责任。

申请权限最小化。业务无关权限的授予会导致权限的滥用，增大应用攻击面，引入用户敏感数据泄露风险。应用应遵循合法正当必要原则，只申请业务必要的权限。对于SDK等外部代码的引用，开发者应保证其相关权限的申请同样满足最小化原则，限制SDK过度申请权限。在实践方面，开发者在开发应用时，不应在启动时申请所有权限；不应申请与业务功能无关的权限，不使用的权限要及时清理；在存在替代功能实现方式的情况下，不应以提升用户体验为由，强迫用户授予权限；不应在业务功能不必要的情况下，滥用自启动权限。

按业务功能分项动态申请权限。开发者应遵循最小化原则，按业务功能分项动态申请权限，仅在使用相关功能时合理申请相应权限。应用应明确告知拒绝授权的后果，用户拒绝授权的，不应影响其他业务功能的使用。

优先采用系统自身功能，代替调用相关敏感权限。例如，应用实现拨打电话功能时，建议采用Intent消息调用电话拨号盘界面，无需额外申请权限；在数据使用方面，Android系统为每个应用程序分配了私有的文件目录和数据存储空间，无需额外申请存储权限；对于获取设备标识的诉求，开发者应采用与业务相符的其他替代方式标识用户终端，无需申请读取手机状态和身份（READ_PHONE_STATE）等权限，避免直接获取硬件标识符；涉及资金或财产安全的支付类业务，如收集设备标识码，须向用户提供具有法律效力的用户隐私协议，明确设备标识码的使用范围和保护责任。

（四）采用单项同意获取敏感信息收集使用授权

未经用户同意，应用不得收集使用用户个人信息。征得用户同意应采用概括同意和单独同意相结合的方式，选择适当的同意时机和同意形式，以清晰易懂的方式告知并征求用户同意。

告知同意应遵循的基本原则。

合法原则。应用应遵循法律法规要求收集使用个人信息，不得通过告知或声明以外的方式收集使用个人信息；不将收集的个人信息用于未经告知的目的；不以欺骗、误导、强迫等非法手段收集使用个人信息；不得违反双方约定收集使用个人信息。

正当原则。不采用一揽子同意的方式征得用户同意，不应存在不同意不让用的问题。当用户拒绝收集使用某项敏感信息或不授予某敏感权限时，不影响提供其他业务功能服务。

必要原则。遵循最少够用原则收集使用用户个人信息，收集的信息为提供业务功能服务所必须。不收集其提供服务所必需以外的用户个人信息。

告知方式可采用概括同意和单项同意相结合的方式。

概括同意。应用首次使用时，可通过隐私声明等形式获取用户对一般个人信息收集使用的同意授权。隐私声明应明确告知用户收集、使用信息的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果。

单项同意。收集使用用户个人敏感信息的应用，应在收集敏感信息或调用敏感权限时，通过弹窗或界面等形式进行即时性告知，分别

征得用户的确认同意。个人敏感信息的单项同意应清晰说明关联业务功能收集使用个人敏感信息的必要性，用户拒绝单项同意授权的，应明确告知拒绝提供的后果。应用开发者不应采用一揽子同意的方式征得收集使用用户个人敏感信息的授权，在未获得某单项同意授权的情况下，不应停止提供其他业务功能服务。

告知内容。个人信息的收集及使用公开透明，应通过显著且便于理解的方式，告知用户收集、使用信息的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果。应在客户资料或界面中提供隐私声明，并通过显著方式对重点条款进行突出呈现。同时，提供对用户同意和撤销同意行为进行记录的机制。留存同意记录的内容包括但不限于用户身份、同意时间、同意内容等。

告知时机。应用首次运行时，可征得用户对采集一般个人信息的授权同意；当收集个人敏感信息或调用敏感权限时，可通过弹窗或界面等形式，进行即时性告知，征得用户的单项同意。用户个人信息的使用目的和收集范围，不应超出隐私政策的声明，当收集使用的内容、目的、方式、范围发生变更时，应及时更新隐私声明，显著提示并重新告知用户。重大变更包括但不限于：收集内容增多、收集方式改变、使用目的变化、使用范围增加等。此外，应用下载、升级及修改系统或其它应用配置时，应征求用户同意。

撤销同意。在征得用户概括同意和单项同意时，应用开发者应明确告知用户撤销同意的渠道和方式，并为撤销同意提供便利，包括但不限于在应用“设置”中进行操作。用户撤回某单项同意不得影响其

他业务功能的正常使用，用户撤销同意之后，不再继续收集和处理相应的个人信息。

再次同意。收集使用用户个人信息超出用户同意范围的，应再次告知用户并征求用户的同意。应用开发者若扩展信息使用范围，将用户数据用于精准营销、用户画像、市场调查等未告知用户的场景，需再次征求用户的单项同意。并提供随时撤销同意的机制。

（五）采用加密机制传输敏感数据

采用加密机制传输敏感数据。用户敏感数据的网络传输，应采用安全传输通道和双方身份认证。如金融类等用户数据敏感程度高的业务，应使用 SSL/TLS 等安全传输协议，通过数字证书等机制，认证传输双方身份。同时，应减少不必要的服务接口暴露，降低被攻击的可能性。

实现加载内容的过滤和 URL 的访问限制。随着 HTML5 技术的推广，WEB 应用和混合应用数量增多。应用对于 WEB 技术的使用，应实现加载内容的过滤和 URL 的访问限制，避免跨站脚本攻击（XSS）、远程代码执行（RCE）等漏洞的影响。

（六）谨慎使用外部存储区域

应用在收集和使用用户个人信息时，应加密存储用户敏感数据，保障存储安全。

用户敏感数据应存储在设备的内部存储中。存储区受应用沙箱保护，其他应用无法访问沙箱内文件。应用卸载后，设备删除内部存储

中保存的所有文件。

开发者应谨慎使用外部存储。终端设备的外部存储可用于不同应用间数据共享，开发者应谨慎使用外部存储，做好完整性和可用性的校验，避免将用户的敏感数据写入外部存储。

（七）贯彻全生命周期安全编码原则

开发者在应用开发中，应保障代码及用户数据的机密性、完整性和可用性，将安全编码原则贯穿整个软件开发周期。

外部数据处理时应经过合法性校验。开发者在使用外部数据过程中应注重合法性校验，不能假设任何外部数据符合预期，外部数据必须经过严格判断后才能使用。

减少代码的攻击面。代码的实现应尽量简洁，减少与外部环境多余的数据交互。过多的攻击面增加了被攻击的概率，尽量避免将程序内部的数据处理过程暴露到外部环境。

注重SDK等第三方代码安全。应用开发时应保证相关库文件及时更新，并使用服务的最新版本。同时开发者需要对引入的第三方代码进行有效审核，避免旧版本漏洞和外部代码安全问题威胁用户权益。应用集成第三方SDK时，应谨慎使用“交叉唤醒”功能，避免应用间互相启动，长期活跃于终端后台，浪费手机资源。

通过防御性的编码策略弥补潜在的安全风险。由于外部环境的不确定性，以及开发者经验、习惯的差异，代码的执行过程很难完全符合预期设想的情况。在编码过程中应采用输入数据校验、容错设计、异常状态恢复、超时和有限重试设计等防御性编码策略，缓解由于开

发者失误导致的缺陷。

五、应用分发个人信息保护的分析与建议

应用分发平台是指为用户提供应用推荐、搜索、安装、管理、分享服务的网站、应用商店等，是用户获取应用的主要来源。应用分发平台应遵循国家法律法规要求，切实履行主体责任，加强应用管理，开展全生命周期监管，制定完善的开发者政策和分发协议，落实开发者及应用资质审核要求、建立应用上架审核检测、应用相关信息明示、用户投诉与反馈和应用下架等机制，为用户提供安全、优质、便捷和实用的互联网信息服务。

（一）制定完善的开发者政策和分发协议

应用分发平台应在公开、公平、公正的前提下，基于法律法规要求，制定完善的开发者政策和分发协议，明示开发者资质审核要求、应用上架审核检测要求和应用下架规定，以便使开发者清晰了解政策规定和平台要求，提交符合规定的应用，形成良性发展和互动。

（二）落实开发者及应用资质审核要求

应用分发平台应审核开发者资质，与开发者签订服务协议。通过协议声明，告知开发者应履行的权利和义务，登记应用提供者、运营者、开发者的真实身份、联系方式等基本信息，同时审核上架应用的备案、经营许可、知识产权和版权等法律法规要求的信息。

（三）完善分发平台上架机制

应用分发平台应制定明确的上架要求并建立完备的检测机制，通过自动化检测和人工审核手段，对应用收集使用用户个人信息的行为进行规范。在提交应用审核时，分发平台应要求应用提供者声明其获取的权限及用途，并审核应用是否按照最小化原则，申请和使用权限；应用分发平台应基于保护用户知情权和选择权的原则，审核隐私政策和收集使用用户信息的行为；应检测和审核应用是否存在恶意行为，是否具备基本安全防护措施。检测和审核未通过的，应用分发平台应拒绝其上架。

（四）充分明示应用相关信息

应用分发平台应在应用下载界面显著位置明示应用基本信息、开发者信息和申请权限列表及用途。应用基本信息包括包名、版本号、更新日期、大小、适用系统版本等；应用开发者信息包括应用开发者公司或个人、应用运营者公司或个人等信息。同时，应用分发平台应为应用开发者明示信息采集使用的种类、目的、方式和范围提供便捷等展现方式。

（五）探索应用运行期管控方案

应用分发平台应主动探索应用运行期管控和保障方式，探索合理、高效、公平的应用运行期管控方案，可与终端侧开展协作联动，监测应用的不良行为，在应用全生命周期保障用户的合法权益。

（六）建立投诉与反馈通道

应用分发平台应建立通畅的投诉与反馈通道，可通过即时通讯用户组群、网站、手机客户端、400 热线和论坛等多种途径。及时接收用户及开发者的建议和投诉。应用分发平台收到投诉后，应通过既定流程，及时处理反馈用户投诉和应用侵权审核情况，降低不良应用对开发者和用户合法权益的侵害。

（七）建立应用下架响应机制

应用分发平台应提供下架通道，应用开发者可以主动提出下架申请，应用分发平台审核通过后，执行下架操作。分发平台应对应用进行跟踪监测，包括**定期复查**，定期对已上架的应用进行复查，发现问题立即下架；**随时抽检**，随时对重点应用类别如：直播、交友、视频、论坛和新闻资讯等进行抽查，发现问题立即下架。建立应用下架响应机制，及时下架违法违规应用。

（八）定期报送行业监管数据

应用分发平台承担连接用户、应用及终端的桥梁责任，是用户个人信息保护工作的重要环节。《电信业务经营许可管理办法》第二十九条规定，电信管理机构建立电信业务市场监测制度，相关电信业务经营者应当按照规定向电信管理机构报送相应的监测信息。应用分发平台应按照相关标准要求向行业主管部门报送数据，支撑主管部门开展市场监测工作，辅助主管部门进行监管和决策。报送数据包括平台统计、应用基本情况、开发者黑名单、不良应用监测结果等信息，其

中对于用户举报数据，应在保护好举报人个人信息的前提下，共享给行业主管部门。

六、消费者个人信息保护建议

（一）选择信息明示清晰的手机、应用和下载渠道

在购买手机前，通过官方网站、公众号等方式查看预置软件信息。包括名称、功能描述、卸载方法、开发者信息、软件安装运行所需权限列表及用途，以及应用收集使用用户个人信息的内容、目的、方式、范围和隐私政策等。同时，了解手机权限管理及应用功能，权限管理功能是否完善、清晰、易用，建议优先选择从应用和权限两个角度进行分类权限管理的手机。

选择官方或正规的应用下载渠道，查阅应用下载渠道是否充分明示应用相关信息。包括名称、功能描述、开发者信息、软件安装运行所需权限列表及用途，以及应用收集、使用用户个人信息的内容、目的、方式、范围和隐私政策等。涉及收费的应用，是否明示收费标准、收费方式，明示内容是否真实准确、醒目规范。查阅该下载渠道是否具备应用的审核及安全检测机制，是否具备完善的用户举报投诉处置措施等。

在选择下载应用前，重点查阅应用安装运行所需权限列表及用途。以及应用收集使用用户个人信息的内容、目的、方式、范围和隐私政策等。对比不同应用的权限申请和信息收集使用情况，优先选择申请权限少、用途清晰明确、信息告知充分和收集使用范围窄的应用。

建议选择 API 等级 26 以上，经过审核及检测的应用。

（二）使用前充分了解权限管理机制和隐私政策

仔细阅读开机向导内容。在首次使用手机时，仔细阅读开机向导中的隐私政策及用户协议内容，充分了解手机权限管理机制，根据自己的需求慎重选择相应的选项。

充分了解应用收集使用信息。在首次打开应用时，仔细阅读应用弹窗中的隐私政策及用户协议内容，充分了解应用申请权限和收集使用信息的情况，慎重同意个人敏感信息的收集使用。

谨慎授予应用权限。应用安装时，不要一次性授予所有权限，要谨慎授予敏感权限，约束获取位置信息、读取手机号、读取短信记录、读取通话记录、读取通讯录、打开摄像头、使用话筒录音、发送短信、拨打电话等行为。

不要 ROOT 手机。手机 ROOT 后，可能会破坏系统个人信息保护机制和功能，加大了用户个人信息泄露的风险，严重威胁用户的隐私数据以及支付等功能的安全性。

（三）善于使用手机设置功能，增强安全意识

设置锁定方式。为加强手机保护，可选择口令、图案、指纹、人脸或其他身份认证方式来设置开机和锁屏密码，开机或唤醒屏幕时，采用相应方式解锁设备，防止在用户不知情的情况下，数据被他人窃取和盗用，危害用户权益。

启用权限管理功能。启用权限管理功能，在需要时开启或关闭指

定应用的权限，防止手机数据被收集和篡改，造成隐私泄露、流量耗费、费用损失等风险。

启用查找我的手机。可启用类似“查找我的手机”功能，以便用户在手机遗失或被盗等情况下，远程查找、锁定手机和清空手机数据。

合理设置通知。应用通知可能包含用户个人信息，建议在使用手机时善用通知功能。用户可根据自己的需求，在不同的应用场景下，选择合理的通知方式。

定期备份用户数据。推荐用户定期备份数据，在出现遗失或故障等情况时，可及时恢复。

定期升级系统版本。定期更新系统版本，及时修复系统漏洞，保障系统安全性。

重视恶意风险提示。重视恶意应用软件、诈骗电话、诈骗短信和恶意站点等风险提示，用户可选择卸载、删除、拒绝、终止站点访问等措施进行风险处理。

不随意接入无线热点。攻击者可通过恶意 Wi-Fi 热点窃取用户个人信息，在公共场所尽量避免接入未知 Wi-Fi 热点，在非使用阶段尽量关闭 WLAN 开关。

七、智能终端产业行动倡议

提升终端产业个人信息保护能力，加强用户权益保护，离不开全行业的共同努力。近年来，工业和信息化部先后发布了《电信和互联网用户个人信息保护规定》和《移动智能终端应用软件预置和分发管理暂行规定》，明确了收集使用用户个人信息的合法正当必要原则，

规范了移动智能终端应用软件预置和分发行为。行业协会和实验室联合产业界也在制定规范、签署行业自律公约等方面进行了有益的探索。随着《移动智能终端应用软件分发服务自律公约》和《移动应用软件高 API 等级预置与分发自律公约》的发布和实施，终端产业个人信息保护协作体系已经初步形成，在此基础上，我们倡议：

（一）落实企业主体责任，保障用户合法权益

严格遵守法律法规，高度重视个人信息保护。终端厂商、分发平台、应用开发者积极落实主体责任，主动适应个人信息保护和数据管理新形势新要求，严格遵守法律法规，贯彻落实个人信息收集使用规定，不断完善企业内部的个人信息保护和数据管理制度，持续优化用户隐私政策，并将个人信息保护的要求贯彻执行到规划、开发、运营等各个环节，积极配合主管部门的监管要求，切实有效维护好用户合法权益。

（二）加强行业自律，探索自治新方式

在行业协会的组织下，全面加强行业自律。行业自律是用户个人信息保护的关键，也是企业可持续发展的内在基础。鼓励在行业协会的组织下，积极开展自律工作，规范技术手段建设，制定侵犯用户权益应用黑灰名单，构建开发者信用评价体系，完善通报下架机制，建立培训认证体系，全面做好自律公约的执行和落地工作。同时配合行业协会在用户个人信息保护和数据管理共享自治方面加大创新力度，积极探索自律新思路、新方法、新途径。

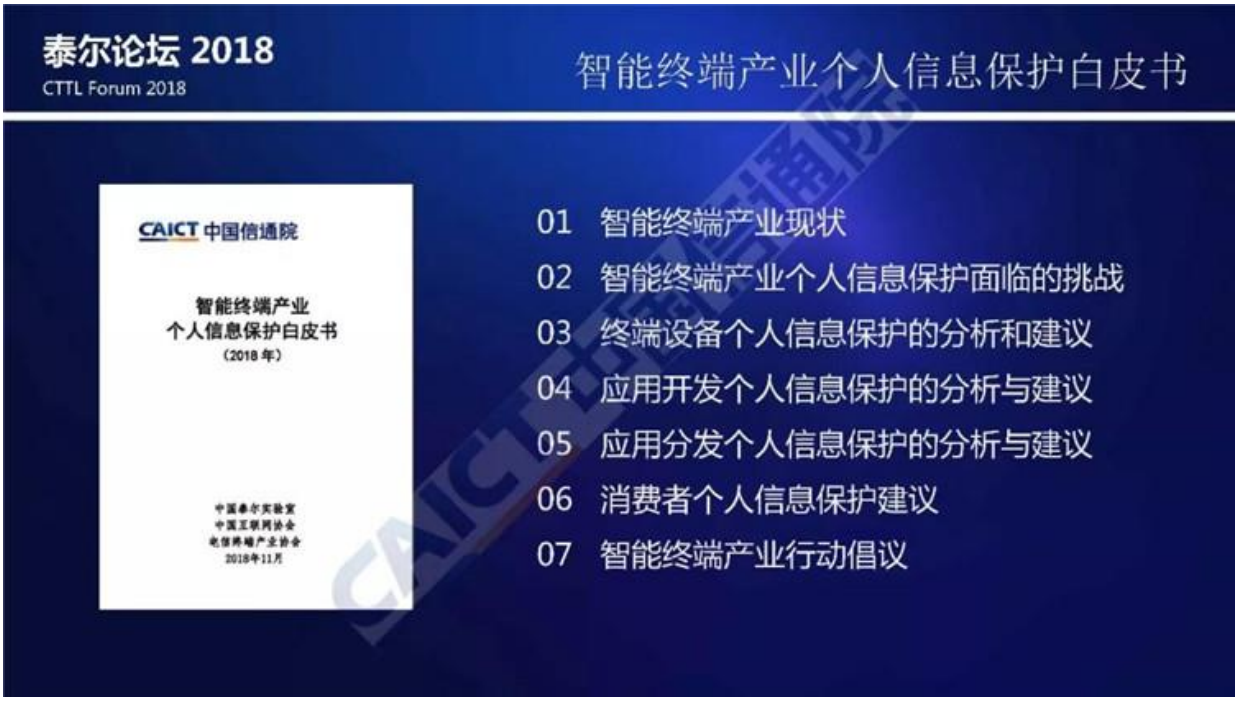
（三）促进公众监督，及时响应用户关切

高度重视用户权益保障，为用户举报监督创造便利条件。公众监督既是手段，也是目的。终端厂商、分发平台应以用户为中心，促进公众监督，为用户举报投诉设置便捷的方式和渠道，健全公众参与监督的机制，时刻关注用户感受和体验，尊重并保障用户的知情权和选择权，积极向行业主管部门移交公众举报信息。

（四）加强沟通协调，强化产业协作体系

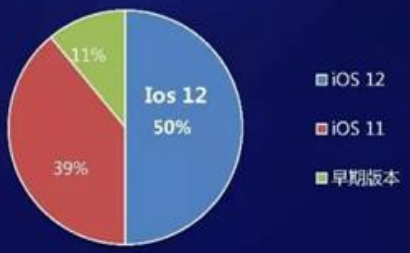
针对焦点和难点问题，产业界齐心协力联手行动。针对当前用户普遍关注的权限滥用和信息过度收集使用等问题，积极响应产业诉求，加强终端厂商、分发平台、应用开发等多环节的沟通协调，在权限管理、告知同意、设备识别码防护等多方面加强协作，制定行业标准规范，研制技术方案，开发检测手段。在检测认证、监测处置等方面协调统一行动，强化产业协作体系，提升终端产业的个人信息保护能力，全民加强用户权益保护。

中国信息通信研究院泰尔终端实验室副主任马鑫对白皮书进行了深度解读。



泰尔论坛 2018
CTTL Forum 2018

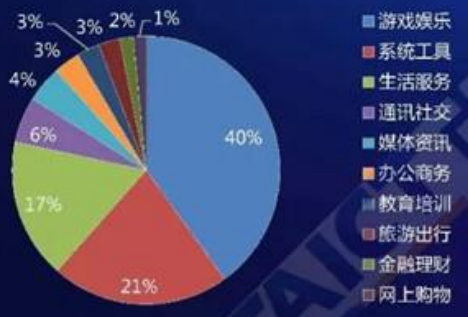
智能终端产业现状



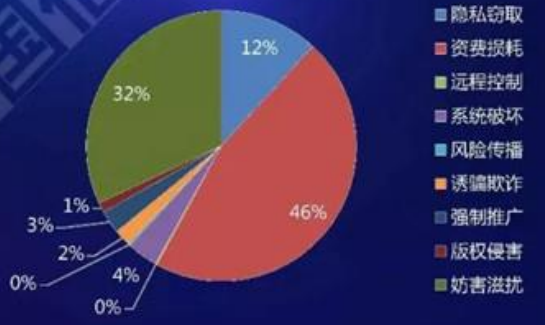
泰尔论坛 2018
CTTL Forum 2018

智能终端产业现状

游戏娱乐类应用风险最高



敏感信息窃取比例 11.86%



泰尔论坛 2018
CTTL Forum 2018

智能终端产业个人信息保护面临的挑战

用户信息过度收集 难识别难举证

- 应用在用户不知情的情况下，过度收集和使用个人信息
- 应用第三方SDK大量收集使用个人信息

权限申请过度 难规范难判定

- 权限申请过度现象严重
- 权限过度申请滥用难规范难判定

低API等级应用规避安卓安全机制

- 低API等级应用风险高，升级难度大
- 近90%的应用API等级在26以下

设备物理识别码防护意识不足

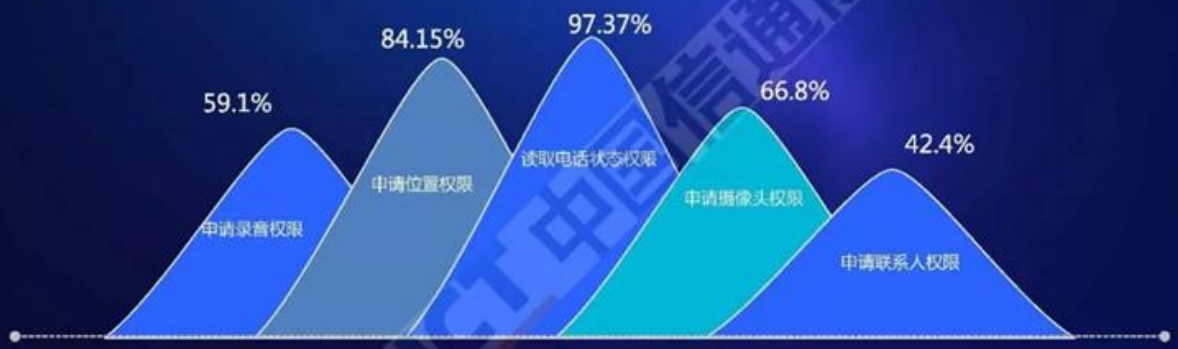
- IMEI、WIFI地址等设备物理地址绑定用户个人身份
- 用户普遍缺乏设备识别码防护意识
- 防护手段不足

隐私与便利选择两难 产业协作能力不足

- 隐私换取便利是无奈之举
- 产业协作能力不足

泰尔论坛 2018
CTTL Forum 2018

权限申请过度现象严重，难规范，难判定



应用权限滥用难规范难判定

根据对国内应用市场TOP 1000应用取样分析显示，Android手机应用普遍会申请与用户个人信息相关的权限，其中，申请写入外部存储权限的比例为99.25%，读取电话状态权限的比例97.37%，申请位置权限的比例84.15%，申请摄像头权限的比例66.8%，申请录音权限的比例59.1%，申请联系人权限的比例42.4%。这种现象表明权限滥用问题普遍存在。过度申请超出应用实际业务功能和场景的权限，为应用过度收集用户信息打开了通道，极易造成用户信息泄漏，威胁用户财产和生命安全。

泰尔论坛 2018
CTTL Forum 2018

终端设备个人信息保护的分析和建议

加大权限调用可知可控力度

- 用户对终端设备权限调用应可知
- 用户对终端设备上权限调用应可控

提高设备识别码防护能力

- 设备识别码匿名化
- 设备识别码替换机制
- 设备识别码要进行严格的获取设置与访问控制

完善应用管控保障机制

- 应用签名
- 运行时内存
- 保护恶意网址检测

落实信息收集使用告知同意

- 在个人信息收集前告知用户
- 告知方式应易于用户感知
- 告知内容应足够清晰且易于理解

重点加强生物特征数据保护

- 生物特征数据应进行加密存储
- 支付环境应采用隔离防护措施

加强基础保障能力建设

- 安全启动
- 强制访问控制
- 内核地址空间布局随机化

泰尔论坛 2018
CTTL Forum 2018

加大权限调用可知可控力度

YD

中华人民共和国通信行业标准

YD/T 2407-2013

移动智能终端安全能力技术要求

Technical requirements for security capability of smart mobile terminal

(ITU-T X.rmsec-4:2012,Security aspects of smartphones,NEQ)

2013-04-25 发布　　2013-11-01 实施

中华人民共和国工业和信息化部 发布

用户对终端设备权限调用应可知

- 终端设备用户的提示可以是图标、文字或其他明显的方式
- 提示应足够引起用户注意，且提示信息易于理解
- 终端设备宜从应用和权限两个视角呈现调用情况
- 建议终端设备提供相应机制，在一定时间内记录并统计应用调用行为情况，可供用户查看详细记录结果

用户对终端设备上权限调用应可控

- 终端设备应通过让用户确认的方式来防范安全威胁，用户应具有选择权，即用户能确认也能取消
- 终端设备未经用户许可不得默认授权
- Android 6.0（API 23等级）及以上，在应用运行时向其授予权限
- 终端设备宜提供应用自启动权限管理功能，用户可设置应用能否被系统或第三方应用启动


泰尔论坛 2018
CTTL Forum 2018
落实信息收集使用告知同意
告知时机在个人信息收集前告知用户
告知方式应易于用户感知
告知内容应足够清晰且易于理解
在企业网站、公众号等渠道明示终端及预置软件的相关信息
用户首次使用时
首次使用功能或服务前、撤回授权后重新使用前
当收集信息发生变更
告知方式，应根据收集的信息类型、功能服务类别、终端设备形态等因素综合考量
告知方式应上创新，如动画、短片等
在通用隐私政策基础上
在终端界面中
在个人敏感信息收集时
告知内容应准确、清晰、易懂，符合通用的语言习惯，避免歧义，不得诱导用户
告知内容应包含收集使用信息的内容、目的、方式、范围、频次、保护措施以及公开、转移、共享等
终端应明示用户对个人信息所拥有的各项权利


泰尔论坛 2018
CTTL Forum 2018
提高设备识别码防护能力
随着设备识别码敏感性的提升，用户高度关注设备识别码被收集滥用的情况。终端设备厂商应加强设备识别码的防护，提升设备识别码防护能力，避免在用户不知情的情况下，与用户身份绑定的物理设备信息被随意收集使用。
设备识别码匿名化
降低因设备识别码泄露用户位置记录、消费习惯等信息的风险。
此外应加快设备识别码匿名化方案的研究，提出切实可行的设备识别码匿名化框架，
提供设备识别码替代机制
终端设备应使用设备识别码作为终端唯一标识符，应提供替代机制。
例如采用广告ID作为唯一标识符，使终端设备应用无法获取设备物理的识别码，用作精准营销、用户画像等。
严格限制获取设备识别码
终端设备应禁止设备直接获取所有的设备识别码
应对设备识别码的访问设置严格权限管控机制

泰尔论坛 2018
CTTL Forum 2018

应用开发个人信息保护的分析和建议

开发者对应用权限申请和个人信息的收集、使用负有主体责任，应在应用的**需求分析、设计、开发、上架、运营、维护和更新**的全生命周期中，高度重视用户个人信息保护工作，全面维护用户的合法权益。

- 采用高等级API开发应用
- 适配最新操作系统及外部代码库
- 遵循合法正当必要原则申请权限
- 采用单项同意获取敏感信息收集使用授权
- 采用加密机制传输敏感数据
- 谨慎使用外部存储区域
- 贯彻全生命周期安全编码原则

泰尔论坛 2018
CTTL Forum 2018

遵循合法正当必要原则申请权限

合理正当必要

开发者在应用设计和开发时，重点关注应用权限的申请和使用，应遵循合法正当必要原则，将最小够用理念贯穿整个开发周期。

泰尔论坛 2018
CTTL Forum 2018

采用单项同意获取敏感信息收集使用授权

概括同意

- 应用首次使用时，可通过隐私声明等形式获取用户对一般个人信息收集使用的同意授权。
- 隐私声明应明确告知用户收集、使用信息的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果。

告知应采用
概括同意和单项同意
相结合的方式

单项同意

- 在收集敏感信息或调用敏感权限时，通过弹窗或界面等形式进行即时性告知，分别征得用户的确认同意。
- 个人敏感信息的单项同意应清晰说明关联业务功能收集使用个人敏感信息的必要性，用户拒绝单项同意授权的，应明确告知拒绝提供的后果。
- 应用开发者不应采用一揽子同意的方式征得收集使用用户个人敏感信息的授权，在未获得某单项同意授权的情况下，不应停止提供其他业务功能服务。

泰尔论坛 2018
CTTL Forum 2018

应用分发个人信息保护的分析和建议

泰尔论坛 2018
CTTL Forum 2018

完善分发平台上架机制，充分明示应用相关信息

完善分发平台上架机制

- 应用分发平台应制定明确的上架要求并建立完备的检测机制，通过自动化检测和人工审核手段，对应用收集使用用户个人信息的行为进行规范。
- 在提交应用审核时，分发平台应要求应用提供者声明其获取的权限及用途，并审核应用是否按照最小化原则，申请和使用权限；
- 应用分发平台应基于保护用户知情权和选择权的原则，审核隐私政策和收集使用用户信息的行为；
- 应检测和审核应用是否存在恶意行为，是否具备基本安全防护措施。

充分明示应用相关信息

- 应用分发平台应在应用下载界面显著位置明示应用基本信息、开发者信息和申请权限列表及用途。
- 应用基本信息包括包名、版本号、更新日期、大小、适用系统版本等；应用开发者信息包括应用开发者公司或个人、应用运营者公司或个人等信息。
- 应用分发平台应为应用开发者明示信息采集使用的种类、目的、方式和范围提供便捷等展现方式

泰尔论坛 2018
CTTL Forum 2018

定期报送行业监管数据

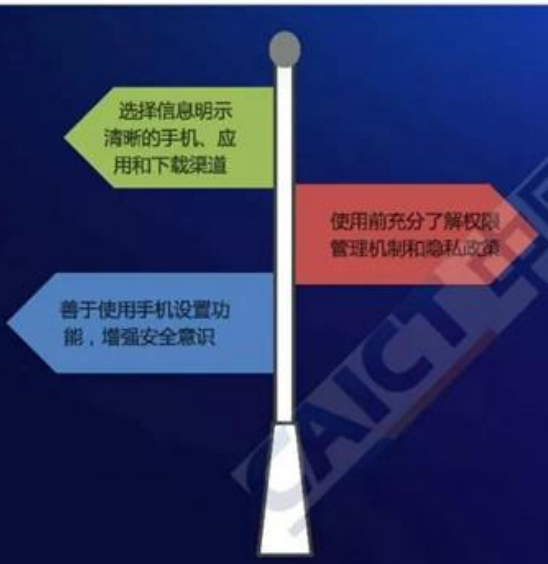
《电信业务经营许可管理办法》

第二十九条规定，电信管理机构建立电信业务市场监测制度，相关电信业务经营者应当按照规定向电信管理机构报送相应的监测信息。

- 应按照相关标准要求向行业主管部门报送数据，支撑主管部门开展市场监测工作，辅助主管部门进行监管和决策。
- 报送数据包括平台统计、应用基本情况、开发者黑名单、不良应用监测结果等信息，其中对于用户举报数据，应在保护好举报人个人信息的前提下，共享给行业主管部门。

泰尔论坛 2018
CTTL Forum 2018

消费者个人信息保护建议



- 通过官方网站、公众号查看预置软件信息
- 选择官方或正规的应用下载渠道
- 查阅应用安装运行所需权限列表及用途
- 仔细阅读开机向导内容
- 充分了解应用收集使用信息
- 谨慎授予应用权限
- 不要ROOT手机
- 设置锁定方式
- 启用权限管理功能
- 启用查找我的手机
- 合理设置通知
- 定期备份用户数据
- 定期升级系统版本
- 重视恶意风险提示
- 不随意接入无线热点

泰尔论坛 2018
CTTL Forum 2018

提升个人信息保护能力，加强用户权益保护
智能终端产业界一直在努力

工业和信息化部

- 2013年7月 《电信和互联网用户个人信息保护规定》
- 2016年12月 《移动智能终端应用软件预置和分发管理暂行规定》

行业自律

- 《移动智能终端应用软件分发服务自律公约》
- 《移动应用软件高API等级预置与分发自律公约》

泰尔论坛 2018
CTTL Forum 2018

智能终端产业行动倡议

1 落实企业主体责任 保障用户合法权益
严格遵守法律法规，高度重视个人信息保护

2 促进公众监督 及时响应用户关切
高度重视用户权益保障，为用户举报监督创造便利条件

3 加强行业自律，探索自治新方式
在行业协会的组织下全面加强行业自律

4 加强沟通协调 强化产业协作体系
针对焦点和难点问题，产业界齐心协力联手行动

泰尔论坛 2018
CTTL Forum 2018

携手共进

共筑终端产业个人信息保护新业态！