刑事司法科学与治理
Criminal Justice Science & Governance
2022 年 第 3 卷 第 2 期

侵犯公民个人信息案件中的手机电子数据应用

皮　浩

奇安信科技集团股份有限公司，上海

摘　要 | 随着信息技术和移动互联网的飞速发展，各行各业普遍通过对公民个人信息进行获取并加以利用以提供更多便捷服务并获利，这样的行为日益成为对公民个人信息安全的潜在威胁，甚至可能带来关联犯罪的发生，严重侵害了公共安全和人民财产安全。电子数据是当今社会公民个人信息最主要的表现形式，拥有多种且大量电子数据信息的智能手机成为主要的存储载体。案件中的手机电子数据即案件发生过程中形成的，通过手机作为载体以数字化形式存储、处理、传输的，能够证明案件事实的数据。手机系统数据普遍存储着大量敏感个人信息，第三方App种类繁多、功能复杂且涉及大量公民个人信息甚至是隐私信息。这些数据信息在采集、传输、使用的过程中是否涉嫌侵权，又或者是否有被窃取和泄露的隐患值得关注。目前，手机电子数据已广泛应用于侵犯公民个人信息案件的证据收集和司法鉴定中，但实践中仍普遍存在数据加密、机身数据提取不全、云端数据提取权限不足、删除数据恢复困难等问题。因此，本文将从保护公民个人信息、打击侵犯公民个人信息犯罪的角度浅谈如何用好手机电子数据证据。

关键词 | 法律；个人信息；手机；电子数据

一、引言

在互联网时代大背景下，信息的收集和获取成为创造社会财富的重要基础，公民个人信息安全已受到潜在威胁。国家通过颁布一系列法律法规不断完善保护公民的合法权益，但是当前公民个人信息主要以电子数据为表现形式、以手机App 为获取手段、以网络为传输途径，如何对侵犯公民个人信息犯罪行为进行精准打击，充分利用关键的电子数据证据显得尤为重要。笔者将结合相关法律法规及专家学者论著，以手机电子数据为视角，探讨电子证据在侵犯公民个人信息案件中的应用。

二、手机电子数据与公民个人信息的概念

（一）手机电子数据

手机电子数据是指基于移动终端应用和通信等电子化技术手段形成的客观资料，一般用以表示文字、图形符号、多媒体等信息，包括以电子形式存储、处理或传输的静态数据和动态数据。

1. 移动通信发展

移动通信技术的发展使得手机已成为人们工作生活中不可或缺的通讯工具，与此同时手机中的电子数据信息量也日益庞大。得益于国内移动通信网络的飞速发展，手机中的数据已经从传统的 SIM 卡、机身存储芯片、内 / 外置存储卡逐步向云端迁移。

目前手机数据的容量已经进入 TB 时代，其中的个人信息数据大致可以分为三类：一是身份验证时输入的鉴权信息，如姓名、证件号码、指纹或者面部特征信息等；二是主动填写的位置信息和被动记录的轨迹信息，如打车记录、地图导航记录等；三是其他授权 App 访问的信息，如手机通讯录、相册等。

2. 数据安全

手机进入智能时代以后，其操作系统经过了十余年的百家争鸣，当下已趋向于由苹果的 iOS、谷歌的 Android 和华为的 Harmony OS 形成三足鼎立的状态。不论哪种操作系统，出于安全考虑，都会设定不同层级的加密和系统权限。通常手机操作系统的底层都是基于 Unix 或者类 Unix 系统开发，系统的管理员账户 root（也称根用户）是唯一的超级用户，因其可对根目录执行读写操作而得名。它具有等同于操作系统的权限，很多系统核心数据（如系统日志）及用户敏感数据（如密码密钥）都需要在 root 权限下才能执行读写操作。因此，手机厂商通常会单独建立一个普通的用户作为日常使用，以规避用户隐私数据泄露的安全隐患。

3. App 的功能与分类

据工信部数据显示，目前国内市场活跃的 App 数量有 300 多万个，包括移动智能终端预置、下载安装的应用软件，基于应用软件开放平台接口开发的、用户无需安装即可使用的小程序。从功能大类来看，主要可分为社交类、新闻类、娱乐类、金融类、生活类、工具类等。

四部门印发的《常见类型移动互联网应用程序必要个人信息范围规定》（以下简称《规定》）对 App 类型做了官方细分，共分为 39 类（见表 1）。

表 1　常见手机 App 功能与分类

序号	App 分类	基本功能
1	地图导航类	定位和导航
2	网络约车类	网络预约出租汽车服务、巡游出租汽车电召服务
3	即时通信类	提供文字、图片、语音、视频等网络即时通信服务
4	网络社区类	博客、论坛、社区等话题讨论、信息分享和关注互动
5	网络支付类	网络支付、提现、转账等功能
6	网上购物类	购买商品
7	餐饮外卖类	餐饮购买及外送
8	邮件快件寄递类	信件、包裹、印刷品等物品寄递服务
9	交通票务类	交通相关的票务服务及行程管理（如票务购买、改签、退票、行程管理等）
10	婚恋相亲类	婚恋相亲
11	求职招聘类	求职招聘信息交换
12	网络借贷类	通过互联网平台实现的用于消费、日常生产经营周转等的个人申贷服务
13	房屋租售类	个人房源信息发布、房屋出租或买卖
14	二手车交易类	二手车买卖信息交换
15	问诊挂号类	在线咨询问诊、预约挂号
16	旅游服务类	旅游服务产品信息的发布与订购
17	酒店服务类	酒店预订
18	网络游戏类	提供网络游戏产品和服务
19	学习教育类	在线辅导、网络课堂等
20	本地生活类	家政维修、家居装修、二手闲置物品交易等日常生活服务
21	女性健康类	女性经期管理、备孕育儿、美容美体等健康管理服务
22	用车服务类	共享单车、共享汽车、租赁汽车等服务
23	投资理财类	股票、期货、基金、债券等相关投资理财服务
24	手机银行类	通过手机等移动智能终端设备进行银行账户管理、信息查询、转账汇款等服务

续表

序号	App 分类	基本功能
25	邮箱云盘类	邮箱、云盘等
26	远程会议类	通过网络提供音频或视频会议
27	网络直播类	向公众持续提供实时视频、音频、图文等形式信息浏览服务
28	在线影音类	影视、音乐搜索和播放
29	短视频类	不超过一定时长的视频搜索、播放
30	新闻资讯类	新闻资讯的浏览、搜索
31	运动健身类	运动健身训练
32	浏览器类	浏览互联网信息资源
33	输入法类	文字、符号等输入
34	安全管理类	查杀病毒、清理恶意插件、修复漏洞等
35	电子图书类	电子图书搜索、阅读
36	拍摄美化类	拍摄、美颜、滤镜等
37	应用商店类	App 搜索、下载
38	实用工具类	日历、天气、词典翻译、计算器、遥控器、手电筒、指南针、时钟闹钟、文件传输、文件管理、壁纸铃声、截图录屏、录音、文档处理、智能家居助手、星座性格测试等
39	演出票务类	演出购票

4. App 的权利与义务

《规定》给予 App 可以获取必要个人信息的权利，所谓的“必要个人信息”是指保障 App 基本功能服务正常运行所必需的个人信息，缺少该信息 App 即无法实现基本功能服务。具体是指消费侧用户个人信息，不包括服务供给侧用户个人信息。

App 存在收集用户个人信息行为的，必须履行《规定》关于“必要个人信息”收集范围的义务，不得因为用户不同意提供非必要个人信息而拒绝用户使用其基本功能服务。法律、行政法规、部门规章和规范性文件另有规定的，依照其规定。

（二）手机 App 中的个人信息

1. App 中个人信息的数据分布

GB/T 35273–2020《信息安全技术 个人信息安全规范》对个人信息的判定提出了两条路径：一是识别，二是关联，并基于此进行了详尽举例。笔者对照前文《规定》中 App 的分类，对 App 中个人信息的数据分布情况进行了分析（见表 2）。

表 2　常见个人信息在 App 中的分布

个人信息分类	涉及的 App
个人基本资料	即时通信类、网络社区类、网络游戏类、学习教育类、本地生活类、邮箱云盘类、远程会议类、网络约车类、网络支付类、网上购物类、餐饮外卖类、邮件快件类、婚恋相亲类、房屋租售类、二手车交易类、交通票务类、旅游服务类、酒店服务类、用车服务类、投资理财类、手机银行类、演出票务类
个人身份信息	手机银行类、网络支付类、投资理财类、二手车交易类
个人生物识别信息	所有支持相应识别功能的 App
网络身份标识信息	所有需要注册登录的 App
个人健康生理信息	问诊挂号类
个人教育工作信息	求职招聘类
个人财产信息	网络约车类、网络支付类、网上购物类、餐饮外卖类、交通票务类、用车服务类、手机银行类、投资理财类、演出票务类
个人通信信息	即时通信类、邮箱云盘类
联系人信息	即时通信类、邮箱云盘类
个人上网记录	浏览器类
个人常用设备信息	实用工具类
个人位置信息	地图导航类、网络约车类、用车服务类
其他信息	婚恋相亲类

2. App 中个人信息的数据生命周期

App数据生命周期包括数据的采集、存储、处理、传输、交换和销毁六个环节。其中个人信息收集的过程又可以分解为明示告知同意、权限申请、本地

获取、本地处理使用、网络传输、对外提供和服务端处理。

明示告知同意通常与权限申请同步出现，通过单一弹窗依次列出所有必要权限一键确认或者逐一弹窗分别确认每一项授权的方式实现明示告知和授权同意。

本地获取数据时，根据不同数据特性分别通过系统 API（如通讯录、位置信息等）、设备属性（如型号、分辨率等）、用户输入（如手机号码、身份证号码等）、用户交互（如浏览记录、支付订单等）等方式实现。

数据获取后，App 对数据进行本地处理使用，数据通常存储在 App 的私有目录下的数据库文件中，数据会经过特定编码或加密处理后使用。

数据通过网络传输时，一般分为四种情况：http 明文传输、http 明文传输加密数据、https 加密通道明文传输、https 加密通道传输加密数据。

对外提供和服务端处理过程可以分为五种情况：通过第三方 SDK 本地获取、App 接入第三方应用收集、App 直接向第三方服务器传输、App 收集数据到服务端后向第三方传输、第三方 SDK 直接采集数据上传到第三方服务器。

3. App 中敏感信息的安全性

App 中的个人财产信息、个人健康生理信息、个人生物识别信息、个人身份信息及其他信息等个人敏感信息在数据收集的过程中，均使用了本地数据加密、网络传输通道加密、二次验证等一种或多种方式，以确保 App 中个人敏感信息的安全性。

（三）法律中的“个人信息”

1. 《刑法》中的“个人信息”

《刑法》在第二百五十三条之一规定了侵犯公民个人信息的犯罪，但并没有解释“公民个人信息”的范畴。而最高法、最高检在 2017 年发布的《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称《解释》）中提出了“公民个人信息”的定义及列举范围，即“以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等”[1]。其后两高一部《关于依法惩处侵害公民个人信息犯罪活动的通知》再次进一步补充。

综上所述，《刑法》中的“个人信息”是指能够识别特定自然人身份或者反映特定自然人活动情况的各种信息。换言之，即公民个人不愿对普通社会公众公开并对其个人有保护价值的信息。

2. “出售、提供、获取”的适用理解

首先，“出售、提供、获取”行为本身侵犯了《民法典》中赋予公民的隐私权，因此属于行为本质的非法，与执行“出售、提供、获取”行为的手段或方式无关。

其次，对于执行“出售、提供、获取”行为的手段或方式，笔者认为，无论是何种手段或方式，只要超越了公民个人意愿对普通社会公众公开的信息范围，且没有获得当事人授权或者许可的情况下，以窃取或者其他方法获取、出售、提供公民个人信息的，即可认定为“非法”。

最后，“出售”从语义上分析，是指将自己获得的信息给予他人并从中牟利的行为；“提供”则是指将自己掌握的不应该提供出去的信息给予他人的行为。换言之，“提供”是不以牟利为目的的给予行为；而“出售”是以牟利为目的的给予行为，应当归属于提供行为。依据《刑法》规定，两者在定罪量刑上并无实质性差异。

3. 《网络安全法》中的“个人信息”

《网络安全法》第七十六条第五款规定了个人信息的定义和范围，其中的“个人信息”与《解释》基本一致，只是在列举时各有侧重。《解释》对财产状况、行踪轨迹等信息作了特别规定，在《网络安全法》基础上就公民个人信息的范围做了进一步厘清。同时顺应当下信息技术及移动互联网的发展趋势，满足打击犯罪的实践需求。

4. 《个人信息保护法》中的“个人信息”

《个人信息保护法》中使用“各种信息”取代了《解释》和《网络安全法》中对相关信息种类的列举，使得受保护的信息范围更加延展。

---

[1] 喻海松．最高人民法院、最高人民检察院侵犯公民个人信息罪司法解释理解与适用［M］．北京：中国法制出版社，2018.

《个人信息保护法》中亦专门对“匿名化处理后的信息”进行了排除。本法第七十三条中对“匿名化”的定义，是指个人信息经过处理无法识别特定自然人且不能复原的过程。笔者认为，排除匿名化处理后的信息，一方面是强调保护的范围，即无法识别或者不可识别特定自然人的信息不受法律保护；另一方面是强调“处理后”，即匿名化处理前的真实信息受法律保护，而处理后的信息不受法律保护。

（四）公民个人信息的边界

1. 个人信息与公开信息

公开的个人信息是指合法公开、能够为不特定第三人所访问的信息，包括个人自行公开和其他合法公开的个人信息两类。信息处理者不经信息主体的同意即可对公开的个人信息进一步处理，但信息处理者对公开信息的后续利用并非不受限制，必须控制在“合理范围”内，受目的限制原则拘束，否则可能引发信息存储、聚合、传播风险，侵害公民的个人隐私权。

在现代社会中，为了实现有效的全方位监管，常常需要信息公开。但是行政机关进行信息公开时需要注意尺度和范围，信息公开不能绝对化，要允许存在例外情况。

因此，笔者认为，自行公开和其他合法公开的个人信息，即使曾经是隐私信息或者敏感信息，也应当被认定为公开信息，从而不再受相关法律保护。

2. 个人信息与隐私信息

个人隐私，即个人信息中的隐私信息，是法律赋予自然人的隐私权中的重要保护内容，依据现行《民法典》相关描述，个人隐私信息是指自然人享有的不愿为他人知晓的私密信息。其中“不愿为他人知晓”属于主观意愿，并不是明确的范围和内容。换言之，如果这部分信息是合法公开的信息，那势必会与个人隐私保护利益冲突。但是部分个人信息对行使知情权和监督权非常重要，因此在具体的法律实践中，只能通过不同的标准来确定个人隐私的界限。笔者认为，个人隐私保护与信息公开的冲突判断标准可以分为以下三种：

第一，社会公众的普遍认知。比如：人们通常将身份信息、家庭信息、财产信息等视为个人隐私。

第二，当事人主动公开。这种情况下相应将信息视为非隐私信息。

第三，公开后会对当事人造成困扰或者负面影响的信息。比如：个人上网记录、工作单位及职务等。此类信息的确认相对复杂，首先，此类信息并没有达到下文所述敏感信息的程度；其次，此类信息可能对不同职业或身份的当事人造成完全不同的影响。

3. 个人信息与敏感信息

个人信息中有一部分信息比较特殊，需要单独拿出来讨论，即个人信息中的敏感信息，简称个人敏感信息。

《个人信息保护法》在定义敏感个人信息时采用了列举，种类中的“等”字，表示列举未尽。即使不在法律明文列举之列，在特定场景下具有敏感性的个人信息也应纳入敏感个人信息的保护范畴。科技的发展及特定场景的变化，也为新型敏感个人信息保护留下空间。同时，将不满十四周岁未成年人的个人信息单列，强调了对未成年人权益的保护，有利于切实维护未成年人的合法利益并促进未成年人健康成长。

综上所述，《个人信息保护法》列出敏感个人信息，区别对待不同种类的个人信息，提高对处理行为的可预测性，明确了企业合规重点，在一定程度上降低企业的合规成本，有利于数字经济发展。

然而，在很多情况下，公开的个人信息与隐私信息、敏感信息确实存在着交叉和转变。笔者认为，个人信息分为公开的信息和不公开的信息，不公开的信息即隐私信息，其中部分特殊的隐私信息即敏感信息。在合法条件下，任何隐私信息和敏感信息都可以转变为公开信息。

三、侵犯公民个人信息案中手机电子数据的应用现状

（一）电子数据取证

1. 电子数据的类型与特点

本文所讨论的电子数据专门指电子数据形式的证据，即电子证据。电子数据是案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据。

除了具有客观性、合法性、关联性这三个证据基本特性外，电子数据还有一些自身的特点，包括

无形性、多样性、易复制性和易破坏性等。

2. 电子数据取证的方法与规范

电子数据取证既需要保证电子数据证据特性的基础技术，又有电子数据取证过程中广泛使用的数据提取、密码破解、数据恢复、数据挖掘、仿真还原、程序逆向、数据分析等相关方法。

我国在电子数据取证领域的研究和实践已经 20 余年，但目前尚无明确的法律法规对电子数据的取证标准进行统一规范施行。国家推荐性标准有 4 个，公安、检察、纪检监察、行政执法等具有取证资格的执法人员关于电子数据取证标准也都是在此规范基础上相互借鉴或者自成一派，仅仅少数组织与部门对取证标准做出了行业适应性规范，例如公安部发布的公共安全行业标准（现行 37 个）、司法部发布的司法鉴定技术标准及规范（现行 19 个）和市场监管总局发布的认证认可行业标准（现行 8 个）。

不同的标准规范会导致后续司法实践中对电子数据审查判断带来不一样的鉴定意见，对证据的证明力乃至案件的定案结论产生影响。电子数据取证标准体系仍需在实践中不断完善，既满足快速发展的信息技术与司法实践的需求，又促进规范化电子数据取证制度的建设。

（二）手机数据取证

1. 手机数据的提取与恢复

手机数据提取通常采取的方式有两种，即备份与逻辑镜像。两种方式都是在开机状态下进行，因此获取的数据不受全局加密机制的影响。备份通常是指利用官方提供的备份工具或者 API 在授权范围内提取部分数据，出于数据安全和存储空间管理等原因，很多系统数据和部分第三方 App 核心数据（包括 App 中的敏感个人信息）都无法备份。逻辑镜像是指在获得系统最高权限后，对完整文件系统进行整体打包或者选择性部分提取。因此，逻辑镜像获取的数据远远多于备份。

基于逻辑镜像或备份从手机中提取的电子数据，借助文件碎片重组、记录还原等手段实现对删除内容的恢复。

2. 手机数据的针对性分析

针对涉及公民个人信息的手机数据分析，主要聚焦在 App 本地记录和 App 行为两个方面。

App 本地记录即 App 在使用过程中存储在本地的数据，通过分析存储在对应数据库表项内的字段内容即可获得，如账号、好友列表、聊天消息、搜索记录、收藏记录、浏览记录等。这些数据以必要个人信息为主，一般不含敏感个人信息。

App 行为即 App 在使用过程中实现获取、传输、对外提供等行为所执行的一系列操作，需要通过静态分析和动态分析两种方式相结合。静态分析一般是通过对反编译技术对 App 进行逆向，分析代码并确定符合行为特征的内容。动态分析一般分为四个环节：一是沙箱行为分析，包括定制 ROM/Hook 框架、污点传播分析、事件模拟、自动点击、界面元素识别、数据关联分析等；二是样本扫描分析，包括第三方 SDK 识别、敏感 API 扫描、权限申请检测、隐蔽行为分析等；三是特征及行为日志分析，包括个人信息相关 API 及调用触发日志、数据存储内容、网络传输内容、权限申请 / 使用日志、用户点击操作记录、用户输入信息等；四是信息获取，包括个人信息类型、获取方式、获取频率、获取及使用场景、传输方式、目的服务器等。

（三）电子数据司法鉴定

1. 电子数据司法鉴定的界定

电子数据鉴定是指鉴定人运用信息科学与技术和专门知识，对电子数据的存在性、真实性、功能性、相似性等专门性问题进行检验、分析、鉴别和判断并提供鉴定意见的活动。电子数据鉴定包括电子数据存在性鉴定、电子数据真实性鉴定、电子数据功能性鉴定、电子数据相似性鉴定。

2. 侵犯公民个人信息案件中的电子数据司法鉴定

在涉及侵犯公民个人信息案件的手机电子数据司法鉴定实践中，通常会涉及存在性鉴定、真实性鉴定和功能性鉴定。核心电子数据来源于功能性鉴定，即通过对手机 App 功能进行分析，找出涉嫌侵犯公民个人信息的电子数据。

四、侵犯公民个人信息案中手机电子数据应用面临的挑战与应对

（一）手机电子数据取证中的安全保障问题

与其他电子数据存储介质不同，手机具有较强的人机交互性，其内部的核心存储芯片很难像计算机硬盘或者 U 盘那样通过只读方式连接在取证工作

站上。即便通过一些设备实现了连接，目前的数据加密也会让后续操作举步维艰。因此，目前通用的手机数据取证方式以开机交互状态下的数据备份和逻辑镜像为主。针对智能手机的取证工作，为保障开机状态下的数据安全，应注意以下几点问题。

第一，确保手机处于信号屏蔽状态或飞行模式（关闭蓝牙、WiFi），防止取证过程中新数据写入、远程锁定或抹除，从而对原始数据造成破坏。

第二，确保手机电量充足，防止因电量不足而意外关机重启后手机无法解锁或者删除数据被清除的情况发生。

第三，确保数据备份不占用 / 覆盖手机机身空间，在取证过程中需确保数据完整性和过程可重复性，特殊情况需对过程详细说明并降低影响。

第四，确保解锁、提权等高级操作下原始数据不被破坏，特殊情况需对过程详细说明并降低影响。

第五，确保 App 动态分析时在模拟环境中进行，防止因真机联网造成原始数据破坏。

（二）手机电子数据加密问题

为了更好地保护用户数据安全，手机厂商陆续启用了全局性的数据加密机制，主要分为两种：FDE（full disk encryption，全盘加密）和 FBE（file-based encryption，文件级加密），只有在开机解锁后才能解密。两种加密方式联合使用，形成双保险。同时，越来越多的 App 对记录数据库进行私有加密，进一步保障了用户个人信息的数据安全，这也令全面提取手机电子数据越发困难。

很多电子数据文件虽然能够被整体提取出来，但囿于其核心内容加密，既无法清晰的分析研判出有效的证据数据，又无法证明相关案件事实，因此无法作为证据使用。为了解决这一难题，技术领域通过不断的研究获得了一些破解之道，但仍然存在无法解密的情况。在这类情况下，只能借助网络通过原有方式登录验证才能看到解密后的明文，然而联网登录验证所带来的数据安全和证据有效性的风险值得重视。

（三）手机电子数据恢复问题

对于已被删除的数据，只有在未被覆盖（含擦除）的情况下才可能被恢复。但手机数据的恢复又存在其特殊问题。

一是文件级恢复，理论上需要获取手机芯片的物理镜像，利用类似硬盘的方式进行数据恢复，但受到 FDE 和 FBE 加密机制、系统管理需求以及闪存芯片存储特性等原因影响，实际上希望渺茫。App 卸载时，一般不会保留原有数据（刻意保留的除外），所有相关文件均会删除，除非能够恢复出数据记录所在的原始文件，否则无法恢复出相关数据。因此，同样需要借助镜像，在未加密的镜像中针对性地恢复 App 目录中的几个核心数据库文件及其他附属文件。恢复出厂时，相当于系统还原，所有数据文件全部清除并被新系统重新覆盖，微信数据几乎荡然无存[1]。

二是记录级恢复，记录数据一般保存在数据库文件中，只要该数据库文件未被删除且数据库内表项未被擦除或者覆盖，就可以通过相应数据库恢复技术进行尝试。

（四）云端数据问题

越来越多的 App 在正常交互中会产生大量的操作日志和用户记录，包括但不限于运行日志、指令记录、连接 / 同步 / 备份记录、轨迹记录、常用地址信息、录像录音、身体特征数据等。这些数据普遍存储在对应厂商的云端服务器中。获取云端数据通常需要云端服务器权限或者分析各设备的网络通讯协议，前者实施的技术难度较小但法律程序难度较大，后者反之。因此，实务界通常采用后一种方式来处理此类情形，在取证计算机上模拟设备与后台通讯，通讯的前提是需要对应的账号和密码来登录，其次可能还需要通过验证码、二维码、图形码或者其他生物特征（如指纹、面部识别等）进行二次验证[2]。然而，由于部分厂商协议和网络数据包的加密，云端数据获取时还需要面临大量繁重的解密问题。

五、结语

电子数据已成为办理侵犯公民个人信息案件的首要证据，但打击侵犯公民个人信息犯罪并不是目

[1] 全国“电子数据与当代法律问题”研讨会．安卓微信取证分析疑难问题研究［C］．西安：西北政法大学，2018.

[2] 皮浩．万物互联时代的电子数据取证［J］．中国信息安全，2019（5）：3.

的，由其引发的网络犯罪链条更加触目惊心。因此，预防侵犯公民个人信息违法犯罪行为的发生，切实保护公民个人信息，杜绝个人信息泄露和非法获取才是重中之重。国家应该督促 App 厂商通过深度检测，将电子数据取证的方法应用到 App 个人信息合规及自身安全问题的整改中，提升 App 的整体安全合规水平，切实解决个人对 App 获取隐私信息的忧虑，推动产业健康、持续发展。

（责任编辑：何　为）

The Separation of the Interest Characteristics of the Interpersonal Information Game in the Virtual Community

Pi Hao

Qi An Xin Technology Group Inc, Shanghai

Abstract: With the rapid development of information technology and mobile internet, the behavior of acquiring and using citizens' personal information has increasingly become a potential threat to the security of citizens' personal information, and may even lead to the occurrence of associated crimes, which seriously infringes on public and people's property security. Electronic data is the most important form of information, many kinds of digital information in smart phones. Electronic data of mobile phones in a case refers to the data formed during the occurrence of the case, stored, processed and transmitted digitally through the mobile phone as a carrier, which can prove the facts of the case System data in mobile phones often stores a large number of sensitive personal information, Apps all have lots of kinds, complexed functions and mass of citizens' personal information and even secret information. It is worth paying attention to whether the data information may be stolen or leaked in the process of collection, transmission and use. At present, electronic data of mobile phones has been widely used in the collection of evidence and forensics of cases of infringement on citizens' personal information, but in practice there are still widespread problems such as data encryption, incomplete data extraction from the chips, insufficient data extraction authority from the cloud, and difficult of recovering deleted data. Therefore, this paper will focus on how to use electronic data of mobile phones with the protection of citizens' personal information and the attack on citizens' personal information crime

Key words: Law; Personal information; Mobile phone; Electronic data