国盟信息安全通报

2019 年 1 月 28 日第 185 期

国盟信息安全通报

（第 185 期）

国际信息安全学习联盟

2019 年 1 月 28 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 375 个，其中高危漏洞 110 个、中危漏洞 236 个、低危漏洞 29 个。漏洞平均分值为 5.86。本周收录的漏洞中，涉及 0day 漏洞 161 个（占 43%），其中互联网上出现“DolibarrERP-CRM 'rowid' SQL 注入漏洞、Ampache 存在多个反射型跨站脚本漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1501 个，与上周（1475 个）环比增长 2%。

主要内容

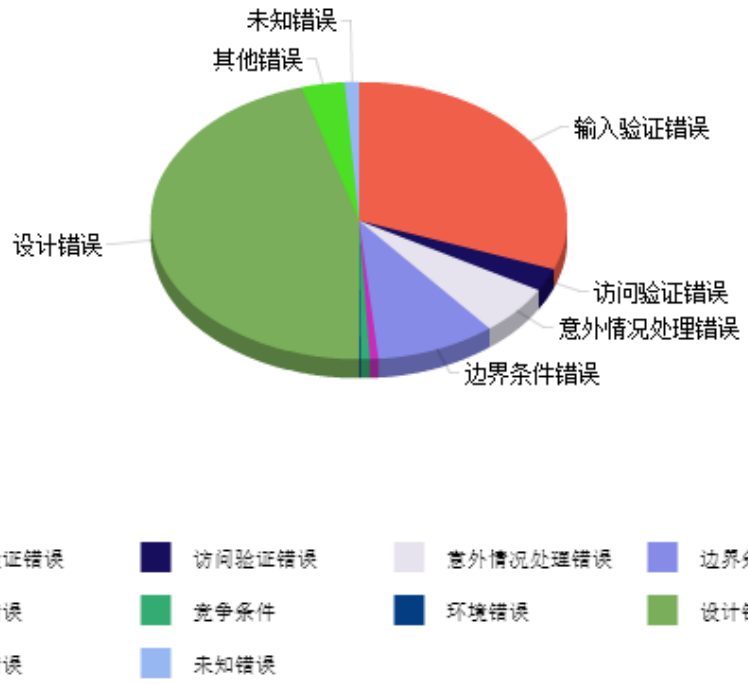
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

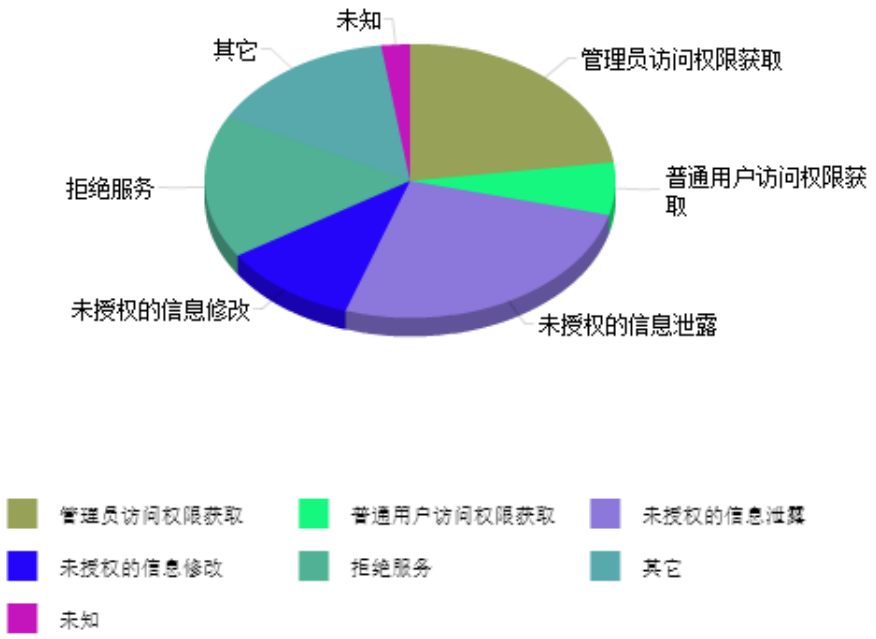
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 375 个，其中高危漏洞 110 个、中危漏洞 236 个、低危漏洞 29 个。漏洞平均分值为 5.86。本周收录的漏洞中，涉及 0day 漏洞 161 个（占 43%），其中互联网上出现“DolibarrERP-CRM 'rowid' SQL 注入漏洞、Ampache 存在多个反射型跨站脚本漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1501 个，与上周（1475 个）环比增长 2%。

二、安全漏洞增长数量及种类分布情况

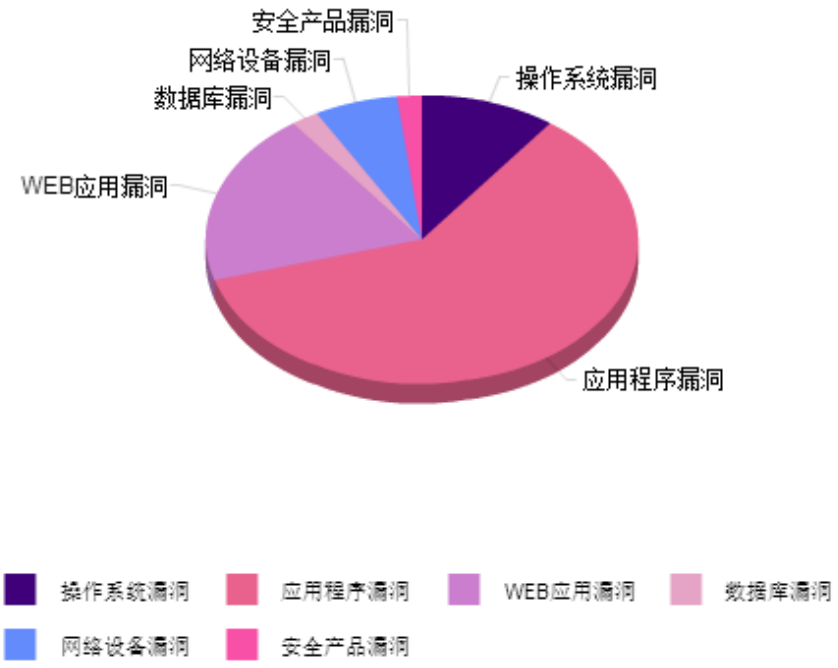
➢ 漏洞产生原因（2019 年 1 月 14 日—2019 年 1 月 28 日）



➢ 漏洞引发的威胁（2019 年 1 月 14 日—2019 年 1 月 28 日）



➢ 漏洞影响对象类型（2019 年 1 月 14 日—2019 年 1 月 28 日）



三、安全产业动态

➢ 筑牢个人信息安全防线

大数据、人工智能等先进技术在服务人类时，不能以牺牲个人隐私为代价。尊重和保护个人信息，不仅关乎技术和商业伦理，更是衡量一个社会文明程度高低的标志之一。

相信不少人都感受过互联网广告的“善解人意”：你在网上无意中浏览了一件商品，之后同类商品就会不断在你的电脑桌面上弹出；网上注册个账号学习英语，一些课程广告就马上充斥邮箱；用手机银行汇一笔款，各色理财顾问就很快致电“问候”……商家之所以能如此及时、准确地了解甚至预知你的需求，并有针对性地投放广告、推荐服务，原因在于他们通过互联网等技术手段，根据用户在浏览、注册时留下的数据信息勾勒出了一个“用户画像”，数据越丰富，“画像”就越精准。

近年来，随着数据的获取、保存和处理成本降低，数据的价值日益凸显，其应用领域也迅速扩展。但值得注意的是，在享受现代科技带来便利的同时，也不能忽略如影随形的安全隐患和隐私挑战。

大数据时代，我们在工作、生活中时时刻刻都在“生产”信息。许多时候，为了获取一定的服务，难免要提供个人信息。在这一过程中，极易产生个人信息扩散、外泄。因此，大数据时代也往往是隐私保护脆弱的时期。就拿电梯广告来说，随着大数据应用向电梯媒介延伸，电梯就可能成为暴露个人信息的新环境和应用场景，增加了隐私泄露风险。试想，如果未来电梯广告会为你量身推送你曾在线上浏览过的商品，你感受到的恐怕不再是便利，而是身处透明“玻璃房”的不适。

当然，我们不能一味反对数据收集。但是，大数据、人工智能等先进技术在服务人类时，

不能以牺牲个人隐私为代价。应该厘清信息收集机构尤其是商业机构使用收集数据的边界。尊重和保护个人信息，不仅关乎技术和商业伦理，更是衡量一个社会文明程度高低的标志之一。随着人工智能、大数据、移动通信等前沿技术的迅猛发展和快速应用，万物互联正日益成为现实，如果没有相应的数据管理和应用规范，未来不单是电梯，家里的客厅都有可能不再是个人信息安全的避风港。

值得欣慰的是，近年来针对个人信息保护的痛点，我国已经和正在出台一系列法律和规范来保障个人信息安全。2017 年 6 月正式实施的网络安全法，就对信息收集使用、网络运营者应尽的保护义务等提出了明确要求。2018 年 9 月，十三届全国人大常委会立法规划向社会公布，个人信息保护法等 69 件法律草案列入第一类项目。这意味着，个人信息保护法被列入 5 年立法规划。为能安心享受高度智能化时代的技术福利，社会公众也应提高安全意识，并和数据采集平台、数据运营商和立法、执法部门共同努力，筑牢个人信息安全防线。（来源：人民日报）

➢ 过度收集个人信息如何破解及国家标准的路径选择

2018 在移动互联时代，如果单从收集环节来看个人信息保护，最突出的问题应是大众应用程序（APP）过度收集用户的个人信息。开发、经营 APP 的网络运营者如违反了《网络安全法》关于“不得收集与其提供的服务无关的个人信息”的规定，掌握了本不该获得的个人信息，一旦发生信息的滥用、误用，或发生了信息的泄露、毁损、丢失，对用户合法权益造成的损害将成倍地放大。

另一方面，数据即石油、数据是黄金，已经成为数字经济的常识。在经济利益的驱使下，网络运营者最大限度地收集个人信息，用于自己的经营活动中。现实中，往往采取以下两条路径：

一是隐瞒收集个人信息的功能、类型、范围等，偷偷地收集个人信息。这方面不仅直接面向用户的网络运营者会这么做（即直接欺瞒用户），那些给 APP 提供功能模块或组件的第三方开发者也会偷偷嵌入收集个人信息的指令或功能，试图“搭便车”收集个人信息（即同时欺瞒 APP 开发者和用户）。

二是强迫用户同意授权其收集个人信息，即通过“一揽子协议”强制用户授权。如果细究起来，“一揽子协议”还可分为两个方面：服务或功能捆绑，以及故意扩大服务或功能所必需的个人信息。面对这样的“一揽子协议”，用户要么只能全盘接受，要么只能退出走人。

现有的法律提出了应对之策吗？目前，在《个人信息保护法》还未出台前，《网络安全法》提出了对个人信息最为完整、全面的保护设计（如下表所示）。

		细分行为	《网安法》对应条款
过度收集个人信息	隐秘收集	直接面向个人用户的网络运营者欺瞒收集行为	22 条第 2 款：“网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。” 41 条第 1 款：“网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。”
		向上述网络运营者提供功能模块或组件的第三方开发者隐瞒收集行为	
	强制收集	服务或功能强制捆绑	无直接对应的条款
		扩大单个功能必需收集的信息类型、数量等	41 条第 1 款：“网络运营者不得收集与其提供的服务无关的个人信息。”

一、对隐秘收集的分析

从图表可知，针对隐秘收集，《网络安全法》有直接规范该行为的条款。无论是直接面向个人用户的开发者（以下简称“第二方开发者”），还是第三方开发者，均需要明示其收集的功能，不能偷偷摸摸地收集。具体情况如下：

如果第三方开发者承当个人信息控制者的角色（即有权决定个人信息处理目的和方式），则第三方开发者所明示的用户有两类，分别是个人用户和嵌入其服务的第二方开发者。此时

明示的方式可以又分为两种：第一种是第三方开发者直接向个人用户明示并取得同意；第二种是第二方开发者在其向个人用户的告知文本中明确点出第三方开发者的存在，明确说明第三方开发者收集个人信息的目的、规则、范围等，并代替第三方开发者取得个人用户的同意。

实践中，在第二种明示方式下，往往个人用户只能一次性给出对第二方开发者和第三方开发者的同意授权，因此存在“服务或功能强制捆绑搭售”（对其分析见下文）的情况，个人用户的同意实际上被架空。

还要注意的是，第三方开发者如果不决定其所收集的个人信息的处理目的和方式，仅仅依照控制者的指令行事，且绝不截留私自存储个人信息另做他用，其仅仅承当个人信息处理者的角色（此处借用欧盟 GDPR 的定义）。此时，第二方开发者在向个人用户的告知文本中，可以自主选择是否披露第三方存在，因为本质上其需要承担的法律责任并不会转移给个人信息处理者。

二、对强制收集的分析

强制收集是民众非常厌烦的问题，但如何破解却又是非常困难的课题。

第一，按照《网络安全法》第 41 条第 1 款的字面表述，可理解为仅要求第二方开发者明示其提供的服务或功能即可（无论这些功能或服务有多少）。

第二，该条款将“必要”作为基本原则，“必要”原则又可以理解为仅提供必要功能（及服务），还可以理解为要求单个功能中仅收集必要的信息。但对于“必要功能”或“必要信息”，开发者往往能提出各种各样的理由来证明必要性，同时由于存在严重的信息不对称，个人用户基本无法辩驳。

第三，当服务或功能捆绑在一起了，或者每个服务或功能所明示的是一种“扩大版”的必要信息后，个人用户面临的是要么接受，要么走人的局面。

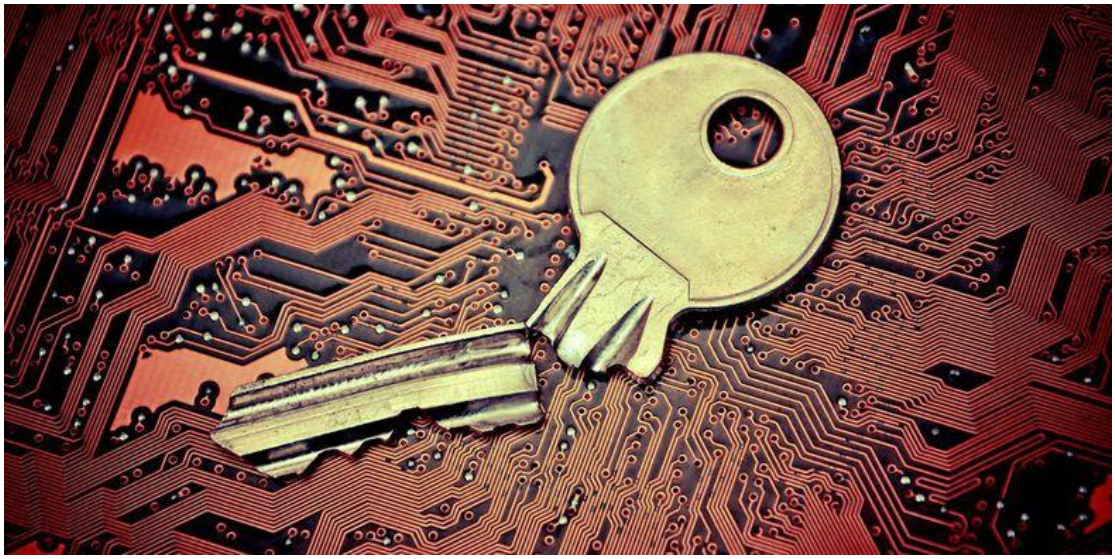
由于存在上述三点，第二方开发者只需要修改隐私政策文本，强制用户点击同意，即在表面上完成了《网络安全法》的合规，就可以大肆收集个人信息了。因此，要防止过度收集个人信息，最重要的议题就是破解强制收集，实际上则是要遏制两种行为：一是强制捆绑服务或功能；二是夸大单个服务（或功能）所必要的个人信息。很可惜，我国现行的法律法规在这方面并没有给予足够的指导。

三、对国外经验的分析

1. 欧盟《通用数据保护条例》

在破除服务或功能强制捆绑方面，《通用数据保护条例》（GDPR）主要通过个人信息处理的合法事由的设计来实现。GDPR 第六条规定了个人信息处理合法的六项事由：一是数据

主体对出于单个或多个特定目的而处理其个人数据表示同意；二是处理是为向身为合同当事人的数据主体履行合同所必需的，或在缔约前，应数据主体的要求所必须采取的步骤；三是因履行数据控制者承担的法律义务而必须处理个人数据的；四是为保护数据主体重大利益或其他自然人重大利益而必须处理个人数据的；五是为公共利益而执行任务，或数据控制者履行赋予的公共职能时，必须处理个人数据的；六是因数据处理者正当利益或第三方正当利益而必须处理个人数据的，但当数据主体的利益或基本权利和自由（特别当数据主体尚未成年时）高于上述正当利益时，不得使用该事由。



个人信息控制者基于特定目的而开始收集个人信息之前，需要事先确定自己所依赖的合法事由，且不能在后期随意更改。而且每项合法事由使用有着严格的限制，不同合法事由后期搭配的个人信息主体的权利也不尽相同。因此，可以说选择合法事由，是个人信息控制者开展业务前最核心的工作。

合法事由的选择，在很大程度上破除了服务或功能的强制捆绑。例如当个人用户要求物流公司送货到其住所时，这是用户主动要求的服务，因此物流公司处理个人信息（个人用户的姓名、地址、电话等）的合法事由是“合同所必需”。这是如果物流公司将其特定时期其收集的个人信息汇总分析，目的是优化其配送服务，此时物流公司不能够再依赖“合同所必需”，转而应该要求“个人信息主体的同意”或者其“正当利益”这两个选项。

换句话说，通过强制个人信息控制者为不同的处理目的（包括目的所涵摄的一系列处理行为）来选择不同的合法事由，GDPR 自然打破了服务或功能的强制捆绑。因为不同功能或服务，很可能需要不同的合法事由，不能混为一谈，一次性征求个人同意。在我国，上述物流公司的例子在目前的商业实践中，基本是将所有的个人信息用途打包在一起，征求个人用

户的同意。

我国目前的法律法规中，关于个人信息处理的合法事由是个人同意，缺乏像 GDPR 那样的设计。因此欧盟破解强制捆绑的路径在我国无法借鉴。

2. 美国 FTC 的路径

美国并没有欧盟上述合法事由的设计，但美国联邦贸易委员会（FTC）事实上区分了三个层次的同意和退出机制，也在一定程度上遏制了功能或服务强制捆绑的问题：

首先，对于个人用户在具体场景中能够合理预期（reasonable expectation）到会被收集、使用的个人数据，可以推定为用户已经明确授权同意。但对于这个场景中按照推定收集所获得的数据，转做他 用，或者提供给与具体场景中无关的第三方做其他用途时，个人用户很可能无法合理预期，这时候还出现以下两种路径：一是对于个人敏感信息，需要用户自主选择同意是否专做其他用途或者提供给第三方；二是对于非敏感信息，用户通过选择退出的途径来行使选择权。

其次，第二方开发者需要收集在具体场景用户可合理预期之外的个人敏感信息时，最开始就需要用户自主选择同意。

再次，第二方开发者需要收集在具体场景用户可合理预期之外的非敏感信息时，需要给用户提供选择退出的机制。

以上三层次的同意和退出机制，均不能免除向用户告知的义务。只不过告知的形式，按照 FTC 的要求，也应该根据符合或偏离用户预期的程度、个人信息敏感程度、时机等方面综合考虑。同时，FTC 还非常强调，当个人用户在市场上选择较少时，服务提供者不得以提供服务为条件强迫用户同意不合理条款。例如用户选择宽带服务时，宽带服务提供者不得强迫用户同意其记录、追踪用户所有的上网行为并用于推送广告目的，特别是用户如选择不同意就不提供宽带服务。

将上述路径对照欧盟 GDPR 的设计，可发现很大程度的重合。在具体场景中符合合理预期，与 GDPR 中的“合同所必需”异曲同工。个人用户自主选择进去某个服务或者功能场景，与用户主动要求签订合同相近。在这样的场景中，用户应当知道，也愿意提供完成服务或功能所必需的信息。

对于这之外的场景，如果是个人敏感信息，美国要求自主选择同意，与 GDPR 中的同意相近。对于非敏感信息，美国要求选择退出，与 GDPR 合法事由中的“正当利益”相近。

但美国 FTC 的路径为中国所借鉴存在困难，原因主要有两点：一是我国法律中并没有明确区分自主选择同意、选择退出、个人敏感信息等实施美国路径所必需的核心概念。二是合

理预期这个概念难以落地，在实践中，（不同群体、特征的）用户、第二方、第三方、监管机构、消费者保护组织、律师、咨询机构、媒体等，对某个场景下合理预期都可能存在各自的理解。这就意味着，作为 FTC 路径中的核心要素，落实起来需要很高的外部条件。我国目前的监管资源和条件（如理解难以统一、管理水平不一、央地同时管辖等）似乎不足以支撑以不确定的法律概念开展个人信息保护的路径。

3. 收费和非收费的路径

国内外具有学者提出可采用区分收费和非收费服务的路径，来开展个人信息保护。该路径基本逻辑如下：

首先，开发者提供服务或功能是有成本的，只能通过对个人用户的信息进行商业化开发利用（目前主要形式是通过推送个性化广告）取得回报，以对免费提供服务或功能进行补贴。其次，如果个人用户愿意付费，贴补开发者提供服务或功能的成本，则开发者就应当避免对付费用户的个人信息进行商业化开发利用。再次，对于不愿意付费的用户，则开发者保持对其个人信息开发利用的权利。

仔细分析上述模式，可知该路径并不避免个人信息被收集。为完成个人用户所需要的服务或功能，个人用户应当同意开发者收集、使用某些类别和数量的个人信息。只不过，由于用户付费了，开发者不得再将提供服务或功能过程中所必需的个人信息转而用于商业化开发利用。

从这个角度看，这个路径和欧盟 GDPR 有很明显的共通之处。为完成用户所需要的服务或功能，都需要允许收集、使用一定的个人信息，类似于 GDPR 中“合同所必需”。但是由于用户付费了，所以开发者不得再向用户提出将信息转于他用的请求，也就是说在收费路径中，开发者不得再采取 GDPR 中“用户同意”和“正当利益”这两个合法事由。

落实上述路径，应主要通过市场竞争的方式细分出愿意采取收费路径的商业模式。因此国内外鲜见通过公权力推行该路径的例子。

四、《个人信息安全规范》选择破解强制收集的路径

在 GB/T 35273-2017《信息安全技术 个人信息安全规范》的制定过程中，标准编制组充分研究了国内现行的法律法规，以及国外破解强制收集的主要路径（如前所述），最终标准编制组决定避免直接照搬国外的做法，而是借鉴国外路径的本质思路，创设出产品或服务核心功能（或称为基本功能）、附加功能（或称为拓展功能）的概念，做出了如下制度设计：

首先，产品或服务应当自行区分核心和附加功能。其次，对于核心功能或服务，个人用户应当允许运营者收集实现该功能或服务所必需的个人信息，否则该功能或服务无法完成。

此时如果用户选择不同意，则允许运营者不向用户提供功能或服务。但对于附加功能，应当允许用户逐一选择是否需要。同时标准要求，“当个人信息主体拒绝时，可不提供相应的附加功能，但不应以此为理由停止提供核心业务功能，并应保障相应的服务质量”。

上述核心功能和附件功能的设计，意在打破“强制收集”的行为。本质上，核心功能仿造了 GDPR 中的“合同所必需”，附加功能仿造了 GDPR 中的“个人同意”。

实践中，企业经常询问如何区分核心和附件功能？这个问题，是打破强制收集的关键。有些投机取巧的开发者会将所有的功能全纳入核心功能的框中，然后还是强迫个人用户授权同意。如此一来，核心和附加功能的区分将流于形式。为避免这个问题，存在两种解决思路：

一是通过市场竞争或者社会监督的路径来解决。比如说，同样是通信软件，有一家企业把核心功能定义得特别大，附加功能定义得特别小；另外一家把核心功能定义得很小，附加功能定义得很大。对如此大的差别，相信一定会有社会监督机构（如消费者保护组织、媒体、高校研究人员等）或监管机构对此展开调查或约谈，要求企业对自己的划分给出合理的解释。如此一来，通过市场上的竞争和比较，逐渐能够形成各行业关于核心功能和附加功能区分的惯例。换句话说，在这个思路下，标准只要求企业自主划分功能，并对划分提出具体、合理的解释，然后交由市场和外部力量来对企业的划分和解释进行监督。概括起来，该思路提倡通过自下而上，形成对功能的合理划分，打破强制收集的行为。

另外一种思路是由标准化机构针对民众经常使用的应用程序，提出各类应用程序的基础功能和拓展功能的划分指引，并提出具体功能或服务所必需收集、使用的个人信息的最小集合。如此一来，指引能够打破前文所述的强制收集所存在两类行为。而且这样的指引，在通过广泛参与、广泛征集意见、反复试点验证的基础上形成，并定期修订更新。虽然指引不具备法律上的强制力，但是企业对于偏离指引的做法，应当承当具体的解释义务。（来源：北京大学法治与发展研究院 洪延青）

➢ 区块链与金融信息安全

金融业务的正常运行，越来越依赖信息技术作为关键支撑。区块链作为一种分布式组合创新技术，可以实现不依赖特定中心、由多方共同参与和维护、基于算法和技术来保证整体可信安全的新型分布式系统。从技术上提供了异构多活、难以篡改、共识一致、智能合约等优势，如加以有效利用，有可能能够从基础上增强现有金融信息系统的安全性。同时，区块

链技术尚未成熟，其自身也存在安全问题，亟待进一步研究和解决。

一、区块链创造了一种新的金融信息安全解决方案

在金融领域，信息安全是重中之重。简单而言，信息安全就是要保护计算机系统，实现保密性、有效性和完整性。传统上，金融信息系统相对封闭，因此信息安全主要针对机构的内部系统，措施也就比较简单，只要通过设立层层水闸式安全防护，对关键性系统和数据进行隔离即可。

然而，随着信息技术与金融服务的深度融合，金融业的计算环境变得更加开放和多元，金融信息系统的潜在威胁也变得更加复杂和多样。比如，不法分子通过恶意软件或钓鱼网站，可以盗取用户的登录密码和敏感信息；通过攻击中心化的服务器，可以大规模盗取用户信息和账户资金；通过操纵僵尸网络等发动 DDoS 攻击，使金融机构系统对外服务无法正常访问；通过勒索病毒攻击，使金融机构无法访问内部数据，尤其是一些重要的核心数据。若再加上多方互联，情况更为复杂，单一机构的风险可能会传染整个金融行业，引发重大金融风险。

所以说，随着金融信息系统从中心化的封闭体系，转向分布式的开放体系，金融信息安全问题日益严峻，需要从机构之间信息系统互联和开放协作的角度，重新考虑信息安全问题。其中的关键要点是，如何在分布式架构下，引入多方参与，发挥多点优势，通过协作机制来增强整体安全性，从而创造技术可信的安全保障。

对此，作为一种新型协作机制，区块链具有技术可信的全新安全特征，可以为新环境下的金融信息安全问题提供一种很好的解决方案。

一是区块链是一个完全分布式的架构，具有天生异构多活，可靠性强的特点。区块链每个系统参与方都是一个异地多活节点，是天生的多活系统。如果某个节点遇到网络问题、硬

件故障、软件错误或者被黑客控制，均不会影响系统以及其他参与节点。例如：对于 DDoS 攻击而言，由于区块链不存在某个集中服务的节点，因此攻击者找不到特定的攻击目标；对于勒索病毒攻击，如果只对单个或少数的系统进行锁定，也不会影响对数据的正常访问。因此，在区块链这种多点多活、对等网络的架构下，传统攻击无法针对特定目标展开，因而其攻击难度和成本大幅提高。

二是区块链的共识和验证机制，可以保证多方数据一致、难以篡改。在传统信息系统的安全方案中，安全依赖于层层设防的访问控制。通过区块链技术，记录交易的数据库任何人都可以访问，但由于巧妙的设计并辅以密码学和共识机制，区块链的数据记录方式使得修改某一数据需要变更所有的后续数据记录，难度极大。实践证明，这样一个数据库可以确保市值达千亿美金的比特币，在全球黑客的攻击下运转稳定。

三是区块链通过智能合约自动执行，提供技术可信的执行环境。智能合约具有透明可信、自动执行、强制履约的优点。参与方共同维护一个系统，职责明确，无需向第三方机构让渡权利，有利于各方更好地开展协作。同时，智能合约可以自动验证交易过程，任何一方受到攻击，其恶意行为会自动被检测，有效阻隔风险在网络的传播。作为信任机器，区块链有望成为低成本、高效率的一种全新的协作模式，形成更大范围、更低成本的新协同机制。

四是区块链技术充分发挥了分布式系统的优势，随着网络规模的增长，其安全性不断提升，其攻击难度和成本不断加大。对于金融机构而言，借助区块链提供的技术可信特征，可建立超越单一主体的多方网络整体安全性，减轻对单一机构自身主体安全依赖，降低了每个参与方的信息安全负担和压力。基于这种开放的网络化环境，用户不再依赖某个特定金融机构内部平台和技术的安全性，区块链上记录的数据的主导权在用户手中。从某种意义上讲，用户对于自身的数据和资产自主可控有了一个质的飞越。

二、区块链技术中的安全问题

诚然，区块链技术具有很多优点，在信息系统安全设计方面，提出了诸多可取之处。但正如所有的计算机系统一样，区块链技术也存在自身的安全问题，并暴露出一些风险，亟待进一步研究和解决。

一是智能合约代码和协议的安全性。以太坊自正式运转后发生多次安全事故，其中最大的一次是 TheDAO 被黑事件。TheDAO 是一个由程序代码管理的自治的风险投资基金，共募集了 1200 万 ETH。黑客利用 TheDAO 智能合约的安全漏洞，从合约管理的 ETH 中划走 360 万个 ETH。最终以太坊基金会不得不进行分叉以解决该问题。

TheDAO 事件折射出两个问题：一是智能合约尤其是公有链的智能合约的安全问题非常

重要，出现漏洞或错误后，无法像中心化系统那样通过关闭系统、集中升级的办法进行修复。而智能合约往往直接管理资金，一旦出现漏洞会直接导致经济损失，因此需要更强的安全措施。目前在这方面的研究热点是把以往应用在芯片设计或者军事控制系统上的形式化验证的方法，应用到智能合约上，以数学证明的方式尽可能避免人为错误。

二是治理机制的安全性。TheDAO 事件还折射出另外一个问题，即现有区块链缺乏一套完善的治理机制，当社区面临重大决策事件时，如何让社区参与进来，以某种机制形成社区意见，最终在区块链上表达出来。这些决策可能是不同的技术升级提案，也可能是 TheDAO 这样的突发事件处理，或者是该区块链某些基础规则的调整。如果缺乏治理机制，只能通过软分叉或者硬分叉解决问题，最终将导致混乱和分裂。

最近比较有趣的一个趋势是，代币持有者投票的链上治理机制再度作为多目标决策机制兴起。通过代币持有者对涉及全网运行的基本共识进行投票，例如：DPOS 机制中的超级节点、协议参数（以太坊 Gas 上限等）、协议升级等。系统根据投票结果自动执行并更新。但这种方式可能会产生某种集中化的效果，可能会对区块链最基本的分布式安全前提造成影响。总体看，关于链上治理机制，仍处于争议和探索的过程中，尚未有统一的意见，需要我们进一步关注和研究。

三是隐私与安全性。区块链通过一种公开透明的验证方式，来使得参与各方可以独立对全网进行安全检测，及时发现潜在威胁和风险事件，并及时阻断并防止攻击行为的扩散。在这种全局账本模式下，如何保护用户隐私，成为业界研究的热点。这方面主要依赖于密码学算法，在公有链中，需要对交易数据、地址、身份等敏感信息进行保护，同时又能让记账节点验证交易的合法性；对于联盟链，在构建隐私保护方案的同时，需考虑可监管性/授权追踪。可以通过采用高效的零知识证明、承诺、证据不可区分等密码学原语与方案来实现交易身份及内容隐私保护；基于环签名、群签名等密码学方案的隐私保护机制、基于分级证书机制的隐私保护机制也是可选方案；也可通过采用高效的同态加密方案或安全多方计算方案来实现交易内容的隐私保护；亦可采用混币机制实现简单的隐私保护。

三、总结与展望

目前看来，区块链若要实现真正落地，支撑实际业务，在技术层面仍需大量改进工作。对于监管者而言，面对不断演进的区块链技术，需要同步考虑相应的法律法规和技术标准，以加强监管，防范风险。（来源：中国人民银行数字货币研究所　彭枫）

➢ 全球网络安全未来或呈现七个趋势

人全球许多知名企业在 2018 年遭遇重大泄露事件，其中最大规模的单次攻击是美国市场营销及数据聚合企业 Exactis 公司的泄露事件，所泄露的个人信息高达 3.4 亿条。未来一年会有哪些网络安全发展趋势?全球网络安全巨头赛门铁克近日发布的网络安全趋势预测显示，随着全球经济增长，数据安全和隐私问题将被摆在更显眼的位置，2019 年及未来，全球网络安全可能呈现七个趋势。

全球网络安全未来或呈现七个趋势

1. 攻击者可能利用人工智能系统作为辅助进行攻击。

近年来，人们期待已久的人工智能技术商用逐渐成为现实，并在许多商业领域中得到应用。现在，网络上销售的各种攻击工具包让攻击者更容易生成新的威胁，可以预见的是，由人工智能技术驱动的攻击工具可以发动更为复杂的针对性攻击。过去，创建高度个性化的攻击工具需要很多人工和花费，但是现在由人工智能技术驱动的工具包所创建的自动化攻击将会极大地降低发动针对性攻击的成本，几乎至零。

2. 防御者可能越来越依赖 AI 技术来应对网络攻击并识别漏洞。

人工智能技术在安全领域的应用也有其积极的一面。现在，威胁识别系统已经在使用机器学习技术来识别新的威胁。不只是攻击者使用人工智能系统来探测漏洞，防御者也在使用人工智能技术进一步强化安全环境，防御攻击。在个人家庭环境，人工智能与其他技术也更有可能帮助个人消费者更好地保护他们的数字安全与隐私。

3. 不断增加的 5G 部署可能进一步扩大网络攻击范围。

2019 年将是 5G 加速发展的一年。未来会有越来越多的 5G 物联网设备直接连接至 5G

网络，而非通过 Wi-Fi 路由器。然而，这一趋势将使设备更容易遭到攻击。以家庭用户为例，物联网设备会跳过中央路由器，从而难以进行监控。此外，在云端备份或传输数据情况也会为攻击者提供大量的新的攻击目标。

4. 与物联网相关的攻击将发展出比海量 DDoS 攻击更危险的攻击形式。

针对控制关键基础设施的物联网设备的攻击数量将不断增加，如配电与通信网络。同时，随着家居物联网设备更为普及，或将看到家居物联网被武器化，例如在严冬通过攻击关闭敌国居民的家庭恒温控制器。

5. 攻击者可能窥视更多传输中的数据。

未来攻击者可能通过新的方式利用家庭 Wi-Fi 路由器和其他安全性较差的物联网设备来进行攻击，其中一种便是利用物联网设备发起海量加密劫持活动，以挖掘虚拟货币。攻击者可能在 2019 年继续专注于基于网络的企业攻击，为其窥视受害企业的经营与基础设施提供方便。

6. 越来越多的攻击者可能会将供应链设为攻击目标。

其中，攻击者在合法软件常规的分发位置植入恶意软件，这种攻击可能发生在软件供应商或第三方供应商的生产过程中。此类攻击的数量与复杂程度均在不断增加，未来可能会出现攻击者试图感染硬件供应链。典型场景可能是攻击者将合法软件更新替换为恶意版本。

7. 日益增加的安全与隐私问题将加强立法与监管活动。

欧盟在 2018 年出台了一般数据保护条例，全球其他国家也正在讨论类似条例的妥善性。几乎能够确定的是，针对不断提升的安全与隐私需求，法律与监管行动未来将会不断升级。与此同时，过于广泛的法规可能会禁止网络安全公司在识别和反击攻击时共享极为普通的信息。如果措施采取不得当，安全与隐私法规会在消除其他漏洞的同时，也可能会衍生出新的漏洞。（来源：中国经济时报）

四、政府之声

➢ 工业和信息化部关于印发《工业互联网网络建设及推广指南》通知

2019 年 1 月 18 日，工业和信息化部日前印发《工业互联网网络建设及推广指南》，明确提出将以加快企业外网络和企业内网络建设与改造为主线，以构筑支撑工业全要素、全产业链、全价值链互联互通的网络基础设施为目标，以企业网络应用创新和传统产业升级为牵引，着力构建网络标准体系、加强技术引导，着力打造工业互联网标杆网络、创新网络应用，着力建设标识解析体系、拓展标识应用，着力完善网络创新环境，规范发展秩序，加快培育网络新技术、新产品、新模式、新业态，有力支撑制造强国和网络强国建设。到 2020 年，形成相对完善的工业互联网网络顶层设计，初步建成工业互联网基础设施和技术产业体系。

各省、自治区、直辖市及计划单列市工业和信息化主管部门、通信管理局，中国电信集团有限公司、中国移动集团有限公司、中国联合通信集团有限公司，各有关单位：现将《工业互联网网络建设及推广指南》印发给你们，请认真贯彻执行。（来源：工信部）

- **《附件：工业互联网网络建设与推广指南》全文：**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c6605619/part/6605652.doc

➢ 四部门关于开展 App 违法违规收集使用个人信息专项治理的公告

2019 年 1 月 25 日，中央网信办、工信部、公安部、市场监管总局等四部门召开新闻发布会，联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》。

近年来，移动互联网应用程序（App）得到广泛应用，在促进经济社会发展、服务民生等方面发挥了不可替代的作用；同时，App 强制授权、过度索权、超范围收集个人信息的现象大量存在，违法违规使用个人信息的问题十分突出，广大网民对此反映强烈。为切实治理个人信息保护方面存在的乱象，四部门决定自 2019 年 1 月至 12 月，在全国范围组织开展 App 违法违规收集使用个人信息专项治理。

《公告》指出，App 运营者收集使用个人信息时要严格履行《网络安全法》规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。遵循合法、正当、必要的原则，不收集与所提供服务无关的个人信息；收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则，并经个人信息主体自主选择同意；不以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反法律法规和与用户的约定收集使用个人信息。倡导 App 运营者在定向推送新闻、时政、广告时，为用户提供拒绝接收定向推送的选项。

此次专项治理将重点开展以下工作：一是组织相关专业机构，对用户数量大、与民众生活密切相关的 App 隐私政策和个人信息收集使用情况进行评估。二是加强对违法违规收集

使用个人信息行为的监管和处罚，包括责令有关 App 运营者限期整改；逾期不改的，公开曝光；情节严重的，依法暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。三是公安机关开展打击整治网络侵犯公民个人信息违法犯罪专项工作，依法严厉打击针对和利用个人信息的违法犯罪行为。四是开展自愿性 App 个人信息安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的 App。

希望广大 App 运营者根据法律法规要求，主动自查自纠，规范个人信息收集使用行为，切实提升个人信息保护水平。（来源：中国网信网）

➢ 国家网信办近期集中清理 7873 款恶意移动应用程序

2019 年 1 月 24 日，据中国网信网消息，2018 年 9 月以来，国家网信办会同工信部、公安部等有关部门发现并清理 7873 款存在恶意扣费、信息窃取等高危恶意行为的移动应用程序，并督促电信运营商、云服务提供商、域名管理机构等关停相关服务。

专项整治期间，国家网信办组织技术单位对在各类网络平台传播的移动应用程序进行巡查，重点检测游戏、壁纸、工具、电子读物等受众广、风险高的应用程序，发现“全民切水果”“浴室女神”等程序通过隐蔽执行、欺骗用户点击等方式订购收费业务，造成用户经济损失；“激情福利社”“调皮女仆”等在用户不知情或未授权情况下，窃取个人信息；“小二轰炸机”“水果忍者大乱斗”等存在向指定用户发送大量短信、捆绑下载、拦截短信等流氓行为。

有关负责人表示，国家网信办将对恶意程序保持高压严打态势，加强日常巡查执法，适时开展专项整治，督促应用商店、网盘、论坛贴吧等网络平台切实落实主体责任，提升安全检测能力，压缩恶意程序生存空间。（来源：国家互联网信息办公室）

➢ 杭州发布城市大脑与政务数据安全管理两项地方性标准

2019 年 1 月 9 日，杭州市数据资源管理局获悉由该局牵头起草的《城市大脑建设管理规范》和《政务数据共享安全管理规范》已于近日正式对外发布。

2016 年 4 月，杭州市以交通治堵为切入口，在全国率先建设城市大脑，城市大脑也于第二年被科技部列为新一代人工智能开放创新平台。通过两年多的建设，杭州城市大脑已从

单一的交通领域延伸到城管、卫健、旅游、环保、警务等领域。

“这两份地方标准，是杭州城市大脑建设的成果之一。有了标准，城市大脑建设也就有了规范。”杭州市数据资源管理局综合协调处副处长黄雪峰说.城市大脑，是一个前所未有的工程，无法从书本里找到建设方案。经过两年多的建设，杭州给出了自己的规范。

《城市大脑建设管理规范》规定了城市大脑建设管理的术语和定义、基本原则、机构及职责、总体架构、能力设计、标准规范、评价与改进。比如，杭州给出了城市大脑的总体架构，包括大脑平台、行业系统、超级应用。此外，《城市大脑建设管理规范》还罗列了 5 条在城市大脑建设管理中需遵循的基本原则，包括整体规划、深度整合，需求为先、慧政惠民，创新驱动、服务产业，政府引导、市场驱动，统一标准、有序推进。

建设城市大脑，政务数据共享的安全性最为引人关注。《政务数据共享安全管理规范》规定了政务数据共享的总则、基本要求、数据归集安全、数据传输安全、数据存储安全、数据处理安全、数据共享安全和数据销毁安全。“从数据归集、传输、存储到处理、共享，再到销毁，这个标准建立了一个严密的管理规范。”黄雪峰说。杭州地方标准的发布，希望能够为其他城市建设城市大脑提供有益的借鉴。（来源：杭州市数据资源管理局）

- **DB3301T 0273—2018 城市数据大脑建设管理规范**
- **全文：**http://t.cn/Et49mWR
- **DB3301T 0276—2018 政务数据共享安全管理规范**
- **全文：**http://t.cn/Et4C4b6

五、本期重要漏洞实例

➢ TP-Link WDR Series 命令注入漏洞

发布日期：2019-01-21
更新日期：2019-01-22
受影响系统：
TP-LINK WDR Series <= 3
描述：

CVE(CAN) ID: CVE-2019-6487
TP-Link WDR Series 是一款 WDR 系列无线路由器。

TP-Link WDR Series v3 及之前版本固件（例如：TL-WDR5620 V3.0 版本），在实现中存在命令注入漏洞，该漏洞源于 get_weather_observe citycode 字段中包含了 sehll 元字符。远程攻击者可利用该漏洞执行代码。

<*来源：vendor
*>

建议：

厂商补丁：
TP-LINK

目前厂商还没有提供补丁或者升级程序，我们建议使用此软件的用户随时关注厂商的主页以获取最新版本：
http://www.tp-link.com/en/support/download/

参考：
https://github.com/0xcc-Since2016/TP-Link-WDR-Router-Command-injection_POC/blob/master/poc.py

➢ IBM Security Identity Manager XML 外部实体注入漏洞

发布日期：2019-01-21
更新日期：2019-01-22
受影响系统：
IBM Security Identity Manager 6.0.0 - 6.0.0.20
描述：

BUGTRAQ ID: 106657
CVE(CAN) ID: CVE-2018-2019

IBM Security Identity Manager（ISIM）是一套身份管理和治理解决方案。IBM Security Identity Manager（ISIM）Virtual Appliance 是 ISIM 虚拟应用程序。
IBM ISIM 6.0.0 Virtual Appliance 处理 XML 数据时，在实现中存在 XML 外部实体注入漏洞。远程攻击者可利用该漏洞获取敏感信息或消耗内存资源。

<*来源：IBM X-Force Ethical Hacking Team
*>

建议：

厂商补丁：
IBM

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://www.ibm.com/support/docview.wss?uid=ibm10794615
https://exchange.xforce.ibmcloud.com/vulnerabilities/155265

➢ Adobe Acrobat 和 Reader 缓冲区溢出漏洞

发布日期：2019-01-21
更新日期：2019-01-22
受影响系统：
Adobe Acrobat Reader DC <= 2018.011.20063
Adobe Acrobat Reader DC <= 2015.006.30452
Adobe Acrobat DC <= 2018.011.20063
Adobe Acrobat DC <= 2015.006.30452
Adobe Acrobat 2017 <= 2017.011.30102
Adobe Acrobat Reader 2017 <= 2017.011.30102
描述：

CVE(CAN) ID: CVE-2018-19722

Adobe Acrobat 是一套 PDF 文件编辑和转换工具，Reader 是一套 PDF 文档阅读软件。
Adobe Acrobat 和 Reader 在实现中存在越界读取漏洞。远程攻击者可利用该漏洞获取敏感信息。

<*来源：Sooraj K S (@soorajks)

链接：https://helpx.adobe.com/security/products/acrobat/apsb18-30.html
*>

建议：

厂商补丁：
Adobe

Adobe 已经为此发布了一个安全公告（APSB18-30）以及相应补丁：
APSB18-30：Security bulletin for Adobe Acrobat and Reader
链接：https://helpx.adobe.com/security/products/acrobat/apsb18-30.html

➢ Microsoft Team Foundation Server 信息泄露安全漏洞

发布日期：2019-01-18
更新日期：2019-01-21
受影响系统：
Microsoft Team Foundation Server 2018 Updated 1.2
Microsoft Team Foundation Server 2018 Update 3.2
Microsoft Team Foundation Server 2017 Update 3.1
描述：

BUGTRAQ ID: 106650
CVE(CAN) ID: CVE-2019-0647

Microsoft Team Foundation Server 是一套应用程序生命周期管理（ALM）工具套件中的源代码管理、项目管理和团队协作平台。
Microsoft Team Foundation Server 2017 Update 3.1 版本、2018 Update 1.2 版本和 2018 Update 3.2 版本，未正确处理标记为保密的变量时，在实现中存在信息泄露漏洞。攻击者可通过创建任务组，利用该漏洞查看其它用户隐藏的变量。

<*来源：Microsoft

链接：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0647
*>

建议：

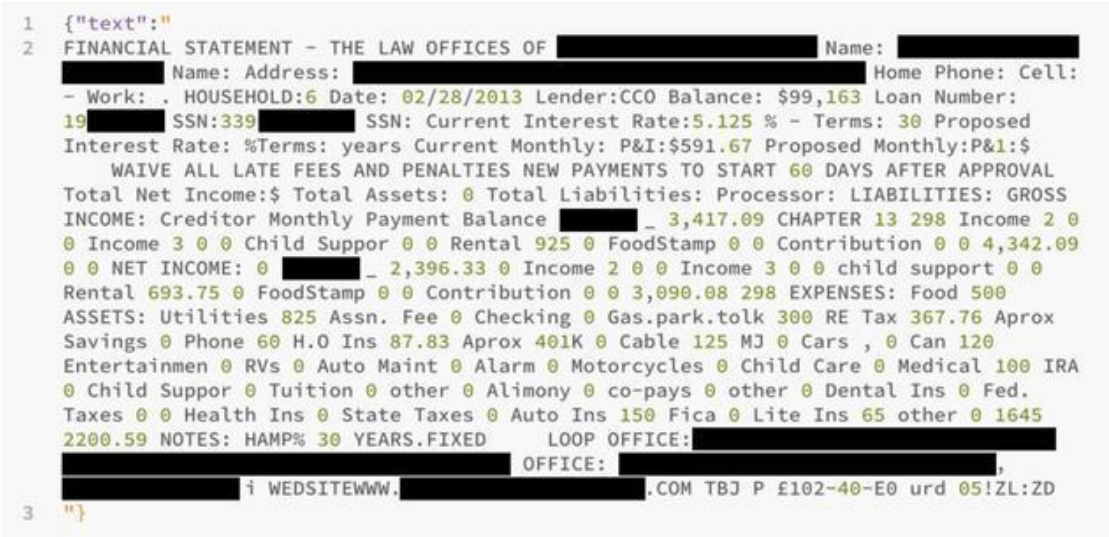
厂商补丁：
Microsoft

Microsoft 已经为此发布了一个安全公告（CVE-2019-0647）以及相应补丁：
CVE-2019-0647：Team Foundation Server
链接：https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2019-0647

六、本期网络安全事件

➢ 涉嫌窃取近千政界人士信息德国 20 岁黑客遭逮捕

2019 年 1 月 24 日，据美国科技媒体报道，因为服务器出现安全漏洞，美国多家大银行泄露 2400 多万份金融及银行资料，涉及大量贷款和抵押贷款信息。受影响的服务器上运行 Elasticsearch 数据库，里面包含了 10 多年的历史数据，比如贷款和抵押贷款协议、还款计划、敏感财务及税务文档。这些文件没有受到密码的保护，任何人都可以查阅。



```
{"text":"
FINANCIAL STATEMENT - THE LAW OFFICES OF [redacted] Name: [redacted]
[redacted] Name: Address: [redacted] Home Phone: Cell:
- Work: . HOUSEHOLD:6 Date: 02/28/2013 Lender:CCO Balance: $99,163 Loan Number:
19[redacted] SSN:339[redacted] SSN: Current Interest Rate:5.125 % - Terms: 30 Proposed
Interest Rate: %Terms: years Current Monthly: P&I:$591.67 Proposed Monthly:P&1:$
    WAIVE ALL LATE FEES AND PENALTIES NEW PAYMENTS TO START 60 DAYS AFTER APPROVAL
Total Net Income:$ Total Assets: 0 Total Liabilities: Processor: LIABILITIES: GROSS
INCOME: Creditor Monthly Payment Balance [redacted] _ 3,417.09 CHAPTER 13 298 Income 2 0
0 Income 3 0 0 Child Suppor 0 0 Rental 925 0 FoodStamp 0 0 Contribution 0 0 4,342.09
0 0 NET INCOME: 0 [redacted] _ 2,396.33 0 Income 2 0 0 Income 3 0 0 child support 0 0
Rental 693.75 0 FoodStamp 0 0 Contribution 0 0 3,090.08 298 EXPENSES: Food 500
ASSETS: Utilities 825 Assn. Fee 0 Checking 0 Gas.park.tolk 300 RE Tax 367.76 Aprox
Savings 0 Phone 60 H.O Ins 87.83 Aprox 401K 0 Cable 125 MJ 0 Cars , 0 Can 120
Entertainmen 0 RVs 0 Auto Maint 0 Alarm 0 Motorcycles 0 Child Care 0 Medical 100 IRA
0 Child Suppor 0 Tuition 0 other 0 Alimony 0 co-pays 0 other 0 Dental Ins 0 Fed.
Taxes 0 0 Health Ins 0 State Taxes 0 Auto Ins 150 Fica 0 Lite Ins 65 other 0 1645
2200.59 NOTES: HAMP% 30 YEARS.FIXED     LOOP OFFICE:[redacted]
[redacted] OFFICE: [redacted],
[redacted] i WEDSITEWWW.[redacted].COM TBJ P £102-40-E0 urd 05!ZL:ZD
"}
```

研究人员相信，数据库只被暴露了 2 周，1 月 15 日又被保护起来。泄露似乎可以追溯到德克萨斯州金融数据及分析公司 Ascension，它提供数据分析、投资组合估值分析服务。在服务过程中，Ascension 将纸制文档、手写文本转化为计算机可以阅读的文件。

Ascension 母公司 Rocktop Partners 的高管证实，服务器出现漏洞，不过系统没有受到影响。1 月 15 日，供应商在配置服务器时出现错误，导致一些与抵押贷款有关的文档泄露。不过供应商很快关闭了问题服务器，Rocktop Partners 正在与第三方专家合作展开调查。

出现问题的供应商叫作 OpticsML。TechCrunch 尝试联系该公司，不过它的网站已经下线，电话也无法接通。（来源：新浪科技）

➢ 拼多多现“优惠券漏洞”事件

2019 年 1 月 21 日，拼多多发布最新情况说明，称上海警方已以“网络诈骗”的罪名立案并成立专案组，并依据“财产保全”的相关规定，对涉事订单进行批量冻结。

拼多多在公告中披露，黑灰产团伙所利用的“优惠券漏洞”盗取的相关优惠券，为拼多多此前与江苏卫视《非诚勿扰》开展合作时，因节目录制需要特殊生成的优惠券类型，仅供现场嘉宾使用。除此之外，此种类型优惠券，从未在任何时候、以任何方式出现在平台正常的线上促销活动当中，甚至从未有任何线上入口。

“该事件中的相关优惠券，均系黑灰产团伙通过非正常途径生成的二维码扫码后获得，该二维码多流传于社交平台相关黑灰产群。”拼多多表示，该非正常途径生成的二维码，原本每个认证信息的用户可且仅可领取一张无门槛 100 元优惠券，而非此前网络流传的单个 ID 可以“无限领取”。

拼多多称：针对这一漏洞，有黑灰产团伙通过“养猫池”(用手机卡蓄养大量虚拟账号)等不法手段，实现 N 张手机黑卡同时作业，批量盗取该种优惠券，并通过手机话费、Q 币等虚拟充值的方式，试图在短时间内迅速转移此类不当所得，涉案优惠券总金额达数千万元。

拼多多表示，目前上海警方已以“网络诈骗”的罪名立案并成立专案组，并依据“财产保全”的相关规定，对涉事订单进行批量冻结。拼多多正配合警方，对涉事订单进行溯源追踪，并最终依据警方的调查结果对相关订单做出依法依规处理。

以下为拼多多公告全文：

拼多多"卫视线下互动专属优惠券"遭黑灰产批量盗取的情况说明：

1、黑灰产团伙所利用的“优惠券漏洞”盗取的相关优惠券，系拼多多此前与一档电视节目(江苏卫视《非诚勿扰》)开展合作时，因节目录制需要特殊生成的优惠券类型，仅供现

场嘉宾使用。除此之外，此种类型优惠券，从未在任何时候、以任何方式出现在平台正常的线上促销活动当中，甚至从未有任何线上入口，这与“某航空公司在官网由于误操作发放低价机票”等事件具有根本性质差异。

2、该事件中的相关优惠券，均系黑灰产团伙通过非正常途径生成的二维码扫码后获得，该二维码多流传于社交平台相关黑灰产群。拼多多从未针对该类型优惠券生成任何二维码，更从未在 APP 及小程序中展示过此类优惠券相关信息及二维码。该二维码具体的生成及传播过程，正待警方调查后获得最终结论。

3、通过该非正常途径生成的二维码，原本每个认证信息的用户可且仅可领取一张无门槛 100 元优惠券，而非此前网络流传的单个 ID 可以“无限领取”。因此，有黑灰产团伙通过“养猫池”(用手机卡蓄养大量虚拟账号)等不法手段，实现 N 张手机黑卡同时作业，批量盗取该种优惠券，并通过手机话费、Q 币等虚拟充值的方式，试图在短时间内迅速转移此类不当所得，涉案优惠券总金额达数千万元。

4、拼多多风控团队负责人表示，黑灰产团伙在盗取金额巨大的优惠券并转移其不当所得后，期望达成“法不责众”的效果，迅速通过网络和社交群将二维码分享出去，诱导一些普通消费者跟风扫码，并在社交平台和群内编造“拼多多平台发券损失 200 亿等谣言”，以希望达到逃避刑责、混淆视听的结果。

5、该事件与此前某航、某电商平台等一系列因 bug 所致资损事件存在本质差别，前者为平台错误操作、非正常发放所致的民事问题，此次拼多多优惠券事件则为“套券诈骗”的网络诈骗案件。打个比方后者类似于犯罪团伙撬开家门实施盗窃之后自己也有些害怕，打开大门招呼更多普通路人进入受害者家中搬取。如按照网络中前者被以“ATM 机误吐钞”现象做类比，后者则相当于非法团伙撬开 ATM 机后实施盗窃。

6、事件发生时正值拼多多“年货节”大促，期间有大批量平台正常发放的优惠券被消耗。至 20 日上午 9 点，遭盗取优惠券和正常优惠券的总和突破平台预设阈值，系统监控到异常并自动报警后，拼多多在第一时间修复了相关漏洞。

7、事件发生后，拼多多迅速向公安机关报案。目前公安机关正在调查过程中，因涉案金额巨大，预计将会对涉嫌套券诈骗、牟取巨额不当利益的涉事黑灰产团伙追究刑事责任。

8、针对该事件，目前上海警方已以“网络诈骗”的罪名立案并成立专案组，并依据“财产保全”的相关规定，对涉事订单进行批量冻结。拼多多平台正配合警方，对涉事订单进行溯源追踪，并最终依据警方的调查结果对相关订单做出依法依规处理。

9、依据目前该事件相关统计及进展，拼多多方面预计，本次事件造成的最终实际资损

大概率低于千万元。此外，期间广为流传的“数十万 Q 币”、“公关部多多哥”、“脉脉网鹿杖客”等相关截图，经查均系不实谣言。

10、本次事件不涉及任何数据安全问题，平台消费者原本正常领取的优惠券使用不会受到影响。为进一步加强“特殊优惠券”相关风控体系，拼多多已成立技术专组。

11、在公安机关的指导下，拼多多将坚决打击黑灰产团伙，不会存在半分妥协与让步。对于遭裹挟的普通消费者，平台主观意愿上不会进行进一步追责，但拼多多不支持此类非正常行为。

12、拼多多平台期间及后续的正常订单，均不会受此事件影响。为充分保障正常参与平台各项活动的消费者的利益，在“年货节”和“春节不打烊”活动期间，拼多多将追加一亿元年货红包津贴，向平台消费者进行发放。（来源：新京报）

➢ 菲律宾金融服务公司数据泄露 影响 90 万客户

2019 年 1 月 20 日，菲律宾金融服务提供商 Cebuana Lhuillier 周六表示，大约有 90 万名客户的数据在未经授权情况下遭黑客窃取，该公司已向有关部门报警并介入这一事件的调查。此次泄密事件发生，正值菲律宾调查人员针对菲外交部长指控黑客入侵该国护照数据库展开调查之际。上周，菲外交部长指控称，一家私人承包的公司从外交部的护照数据库中窃取了文件和数据。

Cebuana Lhuillier 表示，黑客此次针对该公司市场营销部门电子邮件服务器发起的攻击，致部分客户的生日、地址和收入来源等信息外泄。Cebuana Lhuillier 公司提供的服务包括：典当、汇款、小额保险和 B2B 小额贷款解决方案。

“受到影响的只是我们客户的一小部分。而包含 Cebuana Lhuillier 所有客户的主服务器仍然受到保护，且没有遭受攻击。”该公司企业沟通部门主管理查德·维拉瑟兰(Richard Villaseran)表示。他补充说，公司已建议客户如何进一步保护自己的个人信息。（来源：凤凰网科技）

➢ “号码百事通”数据库遭外泄，2 亿余条个人信息被卖！

2019 年 1 月 25 日，前脚买了房，立刻就接到贷款电话;车险即将到期，多家保险公司来电推销……这样的事相信很多人碰到过，背后就是个人信息被非法买卖。但是，最近浙江有一起侵犯公民信息案，从各方面刷新了人们对这个黑色产业的认识——该案非法获利金额累计达 2000 余万元，涉及公民个人信息 2 亿余条。最可怕的是这些信息流出的源头陈某，曾经是中国电信分公司、号码百事通(以下简称“号百”)服务有限公司部门负责人。

流出的个人信息是他从“号百”数据库里获取的，分不同行业、不同地区，相当“专业”。这些手机号码信息，通过层层下线逐渐流向全国 22 个省市。这起案件被全面揭开是不容易的，从一个法律适用疑难的案件入手，到深挖线索、追诉抗诉、并移送线索给有关部门查办，整个过程充分体现了浙江检察机关深化法律监督的职责和作用。

只有手机号没有姓名 算不算侵犯公民信息

2018 年 1 月，浙江省检察院收到来自下级检察院的请示报告，说在办理一起侵犯公民信息案中遇到了法律适用疑难问题。

案件是这样的

陈某甲是一名个人信息的“卖家”，胡某某是其“买家”，曾在陈某甲处购买 30 余万条台州金融类人群的手机号码，无机主姓名。胡某某等人侵犯公民个人信息案件被先行起诉，在庭审中，胡某某及其辩护人就一直强调，购买的信息只是手机号码，单单手机号不构成公民个人信息。后来法院判决认为胡某某从陈某甲处购买的该部分信息不能识别特定的自然人身份，没有对该部分指控予以认定。

在胡某某案件中这部分信息不认定为公民信息，就对检察机关接下来起诉陈某甲造成困扰。手机号码是否属于刑法保护的公民个人信息?陈某甲的行为是否构成侵犯公民个人信息罪?为慎重处理全案、指导后续类案，这个疑问就这样被请示到了省检察院。

从立法精神和司法解释中找到定罪支撑

当时恰逢春节临近，省检察院公诉二处员额检察官王亮、检察官助理赵戬加班加点，审查证据、研究法条、查阅判例。“两高司法解释以定义加列举的方式将手机号码等通讯联系方式明确认定为公民个人信息”“我国已全面实行手机实名制，手机号码与特定自然人相关联，具有专属性和隐私性。”“涉案手机号码针对台州地区有贷款意向的金融类人群，被用于精准营销，更属于公民个人信息无疑”……由此，得出涉案手机号码属于公民个人信息，陈某甲的行为构成侵犯公民个人信息罪，且情节特别严重，依法应于严惩。

浙江省检察院检委会讨论，一致同意承办人意见，认为构罪，而且要求进一步查明犯罪事实，深挖涉嫌犯罪人员。同年 2 月，浙江省检察院发函至省公安厅，建议对陈某甲侵犯公民个人信息案进一步组织侦查。检警双方分别抽调骨干力量，成立专案组。

2 亿条信息来自前“号码百事通”部门负责人

顺着陈某甲这条藤再往上追究，海量个人数据泄露背后的大 BOSS 浮出水面。陈某甲的胞兄陈某乙是上海某教育科技有限公司总经理，原中国电信分公司、号码百事通(以下简称“号百”)服务有限公司部门负责人。

2013 年至 2016 年 9 月，陈某乙从“号百”数据库获取不同行业、不同地区的手机号码信息提供给陈某甲，陈某甲则以每条信息 1 分至 2 角不等的价格，通过网络出售给山东、江苏、吉林等 22 个省、市的“买家”。从 2015 年开始，陈某乙又指使王某帮助陈某甲从“号百”公司数据库获取公民个人信息发送到指定邮箱。两兄弟联手之后的获利相当惊人：累计金额达 2000 余万元，涉及公民个人信息 2 亿余条。在省检察院和省公安厅的联合督办下，办案监督工作取得了重大进展，专案组追诉了陈某甲胞兄陈某乙等同伙及下线 4 人，并将 10 多名下线的犯罪证据移送外省公安机关，同时移送有关部门查处原司法工作人员在本案处理过程中的违法犯罪行为。此外，省检察院还要求对胡某某等 4 人侵犯公民个人信息案提

起再审抗诉。

两位主要被告人都是少见的高学历 面临 7 年以下有期徒刑指控

2018 年 9 月，经指定管辖，温岭市检察院以被告人陈某甲、陈某乙等 5 人侵犯公民信息罪，向温岭市法院提起公诉。2019 年 1 月 3 日，温岭市法院开庭审理本案，庭审从上午 9 点 50 开始，一直持续到晚上 7 点 10 分，公诉人与 5 名被告人及其委托的 7 名辩护人展开激辩。

在诸多侵犯公民个人信息案件中，这起案件中的两位主要被告人也是少见的高学历，比如弟弟陈某甲是硕士研究生学历，哥哥陈某乙是博士研究生学历。“五被告人构成侵犯公民个人信息罪，且情节特别严重，其法定刑为三年以上七年以下有期徒刑，并处罚金。”温岭市检察院员额检察官罗霞在庭上说。案件没有当庭判决。据了解，此前已经一审判决的胡某某等 4 人侵犯公民个人信息再审抗诉案也已开庭审理。

“在大数据时代，侵犯公民个人信息犯罪被称为‘百罪之源’。将涉案手机号码机械解释为单纯的 11 位号码数字，对收集、销售这类号码资源的行为作出不是犯罪的结论，偏离了立法意图，客观上会纵容此类行为的泛滥，不利于社会秩序的构建。”检察官王亮说。（来源：钱江晚报）

➢ 南京警方破获首例技术定位侵犯公民个人信息案

2019 年 1 月 23 日，男子正吃着夜宵，却被讨债人员围住，这是怎么找到自己的？日前，这是国内破获的首例非法侵入手机 APP 获取用户位置信息，为调查公司、讨债公司乃至涉黑涉恶团伙提供人员追踪、技术定位的侵犯公民个人信息刑事案件。该局经过侦查，将开发“APP 神探”定位软件的吴某，以及用该软件非法定位的其他 9 人抓获。目前，吴某及其他犯罪嫌疑人已被公诉。

欠债老板吃饭时被发现一款软件定位聊天位置

2018 年 1 月 20 日，南京市公安局鼓楼分局接到一起报警，一男子称有几个非法讨债人员利用一款手机 APP 定位系统——APP 神探，实时定位了自己的聊天账号位置。他正被堵门讨债，人身安全受到威胁，请求救助。

报警人是在南京做生意的陈某，因到年底了欠了债，这晚在盐仓桥附近一家饭店夜宵时被讨债人员发现，当即将围住。接报后，民警到场进行调查。

陈某说，他愿意还钱，只是想搞清楚，讨债人是怎么找到他的？讨债人很坦诚地说，陈某平时爱用一款知名手机聊天工具，他们就从网上买了一款针对该聊天工具的定位软件，很快就定位出他在盐仓桥一家饭店吃饭，便赶来此地。果然，民警在其中一名讨债人手机里找到这款叫“APP 神探”的定位软件，能对多款主流聊天工具进行实时定位。这一情况引起南京警方网安部门的重视，立刻对其开发者、销售者、使用者等展开侦查。

鼓楼分局网安大队副大队长杨桂年介绍，从初步调查看，这款 APP 软件是针对手机即时通讯工具开发的，通过破解聊天应用程序的安全防护系统，侵入并从中非法获取了被定位对象的经纬度信息，从而非法获知某个人的具体位置，已经涉嫌侵犯公民个人信息犯罪。

经过侦查，2018 年 3 月 26 日下午，南京市公安局网安支队会同鼓楼分局网安大队派员赶往青海省海东市，在当地警方支持下，从一处工棚里抓获了“APP 神探”开发销售者吴某，现场缴获电脑、银行卡等作案工具。此外，还有 9 人因频繁使用该软件非法定位他人位置，也被南京警方抓获。目前，吴某等人已被移送审查起诉。

定位实时误差在 20 至 50 米范围内最低收费 1 元 已有 4000 余人购买

年满 30 岁的吴某是江西上饶人，计算机专业毕业后做起了技术员。他喜欢黑客技术，一个偶然机会看到网上有人卖手机聊天工具定位软件，但使用功能很一般，就想自己开发定位精度更高的。没多久，他破解了一款手机聊天程序的位置信息防护系统，捣鼓出一款新的定位软件，并命名为“APP 神探”，通过 QQ 群、微信群、聊天室等网上渠道销售。

“用户要先在该 APP 软件上注册成为会员，充值后才能使用定位功能。如果对方在线，定位一次只要 1 元；如果对方不在线，定位一次要 10 元。他后来还开发出针对多款主流聊天工具的定位功能，定位一次 100 元。”杨桂年说。

这款 APP 定位精度多高？南京鼓楼网安大队做了多次侦查实验：民警在盐仓桥附近的家乐福超市打开聊天工具，与之相距数公里的同事用该软件进行定位，精确位置只相差 20—50 米。

那么，到底是哪些人在用这款 APP 呢？到案发时，这款定位软件在 2 年间吸引了 4000 多名注册用户，其中充值金额在 1000 元以上的有近 200 人，涉案金额 40 余万元。让人震惊的是，这款定位软件不光被个人非法使用，还成为国内 80 余家调查公司、讨债公司实施不法行为的帮凶，帮其对目标人物实时定位。更可怕的是，国内多个涉黑、涉恶团伙也在用这款定位软件，定位这些团伙要下手的目标人物位置信息，进而实施非法拘禁、故意伤害等违法犯罪行为。

鼓楼分局网安大队梳理 4000 多名注册使用者，成功串并到另一起在南京使用这款定位软件的案件。这是一家涉恶性质的讨债公司，就在鼓楼警方动手前半个月，该公司已被南京雨花台区警方捣毁。

非法入侵手机 APP 获取提供用户定位信息首案为各种手机 APP 技术安全敲响警钟

目前，各种手机 APP 在使用时，都要获取个人通讯、位置等信息的授权。这些个人信息是否得到各个平台安全保护，很多人心中是存在疑问的。

记者在百度上搜索“手机 APP 定位软件”，得到 428 万个结果。可见，瞄上这块蛋糕的，大有人在。如果这些信息被大肆提供给涉黑涉恶团伙，那将会给公民人身安全带来严重的威胁。“这款手机 APP 定位软件的出现，给当前众多手机 APP 软件服务商带来了巨大的风险。”杨桂年指出，当前，手机上的 APP 应用软件大多数的开发原理是基于使用者的地理位置而提供的增值服务。吴某开发的这款定位软件使用的定位技术原理，可以使用在很多 APP 应用软件上，风险极大。

目前，吴某因涉嫌提供侵入计算机信息系统、程序工具罪被移送审查起诉；另有 2 人因频繁非法使用该软件定位他人位置信息，被以涉嫌侵犯公民个人信息罪被移送审查起诉。而在开头陈某案中，使用该软件非法定位并找到陈某的 3 名员工也被依法给予批评教育。

江苏警方表示，作为一种新型犯罪案件，该案的出现对如何有效防范黑客攻击，如何有效保护每个 APP 用户合法权益，既敲响了警钟，又提出全新挑战，应该引起监管部门、APP 服务商和手机用户的高度重视。（来源：法制网）

➢ GDPR 实施后最大罚单：法国罚款谷歌 5700 万美元

2019 年 1 月 22 日，据 TechCrunch 报道法国数据保护监管机构 CNIL 日前按照欧洲《通用数据保护条例》（GDPR）规定，对谷歌开出 5700 万美元(约合 5000 万欧元)罚单。这家监管机构称，在安卓（Android）新用户设置新手机并按照安卓系统的引导流程操作时，谷歌没有遵守 GDPR。这也是 GDPR 实施以来，针对一家公司的最大罚单。

早在 2018 年 5 月，名为“None Of Your Business”(NOYB)和 La Quadrature du Net 的两个非营利组织就已经对谷歌和 Facebook 提出投诉。按照 GDPR 规定，投诉会转给本地的数据保护监管机构。虽然谷歌的欧洲总部位于都柏林，但 CNIL 首先得出的结论是，在为新安卓用户处理数据方面，都柏林的团队没有最终决定权，决定权很可能在山景城总部。

CNIL 随后得出结论，在透明度和获取用户同意方面，谷歌没有遵守 GDPR 规则。

对于缺乏透明度问题，监管机构在报告中写道:“有些重要信息，如数据处理目的、数据存储周期或用于个性化广告的个人数据类别，过度散布在多个文档中，用户需要点击按钮和链接才能获取补充信息。”举例来说，如果用户想知道他们的数据如何被处理以便用于个性化广告，需要点击 5 或 6 次。CNIL 还表示，用户通常很难理解自己的数据是如何被使用的，谷歌的措辞故意宽泛而晦涩。

其次，CNIL 认为，谷歌使用数据前获取用户同意的流程不符合 GDPR 规定。在默认情况下，谷歌会促使用户注册谷歌账户。该公司告诉用户，如果没有谷歌账户，他们的体验

会非常糟糕。CNIL 宣称，谷歌应将创建账户的行为与设置设备的行为分开，这种捆绑行为是违法的。

如果用户选择注册谷歌帐户，当该公司要求用户勾选或取消某些设置时，谷歌不会解释其含义。例如，当谷歌问你是否需要个性化广告时，该公司并没有告诉你它实际上在谈论许多不同的服务，从 YouTube 到谷歌地图再到 Google Photos 等，这不仅仅是关于你的安卓手机。

除此之外，谷歌在你创建账户时不会获取你的明确同意，因为选择退出个性化广告的选项隐藏在“更多选项”链接的后面。在默认情况下，该选项是预先勾选的(尽管本不应该勾选)。最后，在默认情况下，当用户创建帐户时，谷歌在“我同意按照上面描述的方式处理我的信息，并在隐私政策中进一步解释”的框中打上标记。这种广泛的同意在 GDPR 中也是被禁止的。CNIL 还提醒谷歌，自 2018 年 9 月展开调查以来，该公司行为没有发生改变。

NOYB 主席马克斯·施雷姆斯（Max Schrems）发布声明称:“令我们感到兴奋的是，欧洲数据保护监管机构首次利用 GDPR 来惩罚明显违反法律的行为。随着 GDPR 的引入，我们发现像谷歌这样的大公司只是简单地‘以不同的方式解释法律’，往往只是对其产品进行表面上的调整。更重要的是，监管机构必须明确表示，仅仅提出投诉是不够的。令我们感到欣慰的是，我们保护人们基本权利的工作正在取得成果。”

谷歌发言人在声明中称:“人们对我们提高透明度和控制力抱有很高的期望。我们致力于满足这些期望和 GDPR 的同意要求。我们正在研究 CNIL 的决定，以决定下一步的行动。”（来源：网易科技）