中国改革报 CHINA REFORM DAILY
2021.03.26 星期五
本版编辑：孟佳惠 Email：crd_xyzhg@163.com 热线：(010)56805187

美国刑事司法中手机定位信息保护的新发展

□ 卢 莹

在美国，非通讯内容的信息一直被排除在宪法隐私之外。实践中，政府从通讯公司获取手机定位信息已成为侦查犯罪的常态，执法部门藉此重塑嫌疑人的过往行踪寻找其在犯罪现场的证据。嫌疑人事先、事中均不会得知自己成为政府追踪的对象，即便事后获悉，申请法庭排除信息证据、指控政府“非法搜查”的动议往往很难得到法庭支持。近十几年里，已有多起案件涉及执法人员在未取得令状下，获取嫌疑人海量历史定位记录从而引发“非法搜查”的争议，在这些案件中控方用“第三人原则”予以回应，即某人自愿与他人或机构分享的记录或信息不受宪法第四修正案保护。科技革命引发的争议不断升级，美国各界掀起了“获取手机定位信息是否构成宪法搜查”的广泛讨论，直至2018年美国最高法院Carpenter案使争议得以暂时平息。

宪法搜查认定标准的演变

美国宪法第四修正案保护民众不受政府不合理的搜查和扣押，但宪法条文本身对不合理搜查并没有明确界定或说明，因此关于“不合理搜查”的争议案例层出不穷，判断搜查的标准随着社会发展也有所变化。

早期最高法院对该条的解释以保护民众财产权为基础，根据“非法侵入私人财产原则”以物理性侵入作为判断政府行为是否构成宪法搜查的标准。随着科技的大幅进步，当电子技术无须物理性侵入“宪法保护领域”即可产生严重侵犯个人隐私的后果时，传统财产理论已无法为隐私受侵犯者提供适当保护。面对这一问题，最高法院在Katz案将宪法第四修正案保护范围扩展至个人隐私。自此，政府行为是否构成“搜查”之认定标准从“财产权保护”转变为“隐私权保护”，“合理的隐私期待”准则占据主导地位。

在判定合理隐私期待范围时须符合两个条件：一是个人主观上有隐私期待；二是社会客观上认可这种期待是合理的。二者同时满足时，才意味着受宪法隐私权保护。20世纪70年代的Miller案、Smith案确立的“第三人原则”对认定“合理的隐私期待”有较大影响，即个人自愿将信息披露给第三人时，社会客观上不认为个人的隐私期待是合理的，政府从该第三人处获取信息不构成宪法搜查，无须具备相当理由和令状。

Carpenter案前手机定位信息的保护

联邦立法及司法实务。1986年，美国国会通过《存储通讯法案》用于规制已经发生、存储的通讯记录及其他信息，该法规定政府有“特定且明确的事实表明有合理理由相信”信息“与正在进行的犯罪侦查有关且有实质关联”时，可向法庭申请命令强制取得手机定位信息。据此，联邦成文法对定位信息设定的保护标准是“合理理由”，而非宪法保护隐私时的“相当理由”。实践中，“第三人原则”是法庭批准申请的有力依据，使政府可以正当合理地无需令状进行手机定位追踪。2013年，第五巡回法院裁定警方无须搜查令获取手机定位信息。2015年，第十一巡回法院裁定手机定位信息是被告人自愿交由运营商，属运营商所有而非被告，基于“第三人原则”被告人对此没有隐私期待。警方依法庭命令取得的定位信息，并没有侵犯被告宪法权利，不构成搜查。2016年，第四巡回法院也作出类似裁决。

州立法及司法实务。近几年，州立法部门和州法院开始扩张隐私权保护范围，已有8个州明确要求州政府执法人员须有搜查令才能获取手机定位信息。马萨诸塞州最高法院基于本州宪法，认为手机用户对其历史定位信息享有隐私期待，侦查机关须事先取得令状。由于美国各州都有独立的立法权、司法权，因此各州的保护力度存在差异。例如，在明尼苏达州手机定位信息受保护，但在内华达州则不受保护；在新泽西州，警方获取实时定位时需取得令状，但对历史定位则无令状要求；在加利福尼亚州，州警和地方警察均须在令状下获取定位信息，但联邦执法部门则不受此限。

联邦与州采取两套标准，各州之间保护范围存在差别，各民权组织维护定位隐私的呼声日益高涨，如此混乱的局面为美国最高法院核发调卷令提供了充分动机。

Carpenter案情概要及裁判要点

2011年，警方逮捕了4名涉嫌在底特律几家手机商店抢劫的嫌疑人。其中一人承认，在过去4个月里犯罪团伙跨州抢劫了另9家商店。此人确认有15人参与抢劫，并交出自己的手机，警方通过核查识别出抢劫发生前后拨打的电话号码，以寻找漏网之鱼。检察官依《存储通讯法案》取得法庭授权命令，获取被告人长达127天的手机定位历史记录共计12,898条，平均每天101条。

一审开庭前，被告人申请排除定位信息证据，称控方未基于相当理由取得搜查令获取的这些信息违反了宪法第四修正案。地区法院驳回这一动议。庭审中，联邦探员作为专家出庭，利用被告人的手机定位信息绘制其在4起抢劫案中的位置地图，并坚信所有抢劫案发生时，被告人都在犯罪现场附近。陪审团采信这些证据认定被告罪名成立，Carpenter被判处116年监禁。二审第六巡回上诉法院判决维持原判。审判庭遵循“第三人原则”，认为被告对警方搜集的定位信息缺乏合理隐私期待，鉴于手机持有者自愿向运营商传输定位信息以“作为建立通讯的一种方式”，法院认定这些商业记录不受宪法保护。

2018年6月22日，美国最高法院以5:4裁定政府违宪。多数意见采“合理隐私期待”标准，由首席大法官罗伯茨执笔：首先，控方获取被告人手机定位历史信息构成宪法搜查。本案的争议信息并没有完全相同的先例可以参考，虽然与GPS定位追踪有相似之处，但后者涉及的是个人对身体定位和行动轨迹的隐私期待。本案的定位信息属电子数据，且实际上是用户自己传输给通讯运营商的，这就与个人自愿将信息交由第三人的Miller案、Smith案相类似，但后两者能透露的个人讯息相对有限。鉴于争议信息的特殊属性，法院拒绝适用“第三人原则”；其次，法院认定控方在获取被告手机定位信息前并没有基于相当理由取得搜查令。这些记录基于法庭依成文法颁发的命令所得，根据规定政府只需证明至合理理由即可，这一要求与搜查令的相当理由标准相去甚远。因此，属于隐私的手机定位历史信息不能仅凭法庭依成文法发布的命令取得。

多数意见受到了反对派的强烈批评。肯尼迪大法官认为，手机定位信息与根据“第三人原则”获取的其他商业记录并没有什么不同，被告人对这些信息不享有所有权或控制权，因此没有任何隐私期待。他对最高法院将第四修正案与财产权割裂开来表示惋惜。阿里托大法官则建议法院应遵循国会订立的法律，即联邦立法已要求警方在类似情况下无须取得搜查令。托马斯大法官则表示宪法第四修正案无论是条文还是制定过程中均没有“合理隐私期待”标准的存在基础，法庭应重新考虑这一标准。

可以说，本案是数字时代美国最高法院就手机定位信息所作的里程碑式的判决，对隐私扩展至部分非通讯内容的信息而言意义重大。但罗伯茨大法官强调本案适用范围非常有限，如只适用于手机定位历史信息，不适用于其他可能无意中披露定位信息的商业记录。政府可以在紧急情况或涉外事务及国家安全时无需令状收集历史定位信息。因此，本案存有一些未决问题，如宪法第四修正案是否或者如何保护其他类型的信息。最高法院承认个人对提供给第三人的信息可以保有隐私期待，但具体何种信息却没有明确指引；此外，关于获取多长期限的信息会侵犯隐私的问题。本案认为政府获取多于6天的历史定位信息须符合相当理由标准，而6天内的信息则不受宪法隐私保护，法院并没有解释如何得出此结论。这些都会增加实务中的不确定性，引发新的争议。

智利“铁路发展最重要的里程碑之一”

3月23日，智利交通和电信部长乌特参观停靠在首都圣地亚哥的15列中国轨道列车，称赞这批车辆的到来是近年来智利“铁路发展最重要的里程碑之一”。图为智利交通和电信部长乌特(中)在首都圣地亚哥参观轨道列车并出席新闻发布会。

新华社发(豪尔赫·比列加斯 摄)

智能家电或将沦为网络攻击“帮凶”

□ 柳玉鹏 晨 阳

在全球范围内，智能家用电器越来越受到欢迎。人们喜欢将家中的空调、冰箱甚至电热水壶都连接到网络上，尽管这样的设计是为给日常生活提供方便，但它同时也引发意想不到的问题。俄罗斯专家警告称，智能家电正面临着安全问题，一旦遭到黑客渗透，不但可能导致用户信息被窃取，甚至在不经意间成为大规模网络攻击的“帮凶”。

泄露的个人信息范围很广

俄罗斯《消息报》报道称，近年来，世界各国都在积极推进物联网概念，将许多智能新功能嵌入到家电中。从传统的冰箱、空调、电视等大家电，到音箱、灯泡、咖啡机、吸尘器、体重秤甚至电动牙刷等小电器，都可以配备无线接口，以通过网络进行远程激活和数据传输，旨在方便人们的生活。

但这些智能家电设备也带来空前的网络安全漏洞，黑客可以借机拦截用户的任何信息或生物识别数据，具体的跟踪方法因智能设备的类型和传感器而各异。俄罗斯Velter公司首席执行官安德烈·费多罗夫称，具有内置语音助手的音箱可以记录人们的对话，并将音频数据传输到第三方服务器上。内置摄像头的设备能够发送照片和视频数据，而具有GPS模块的设备则可进行地理位置定位。“例如十分流行的Roomba机器人真空吸尘器，它能根据房屋周围的移动情况制作房屋的模拟地图，这些数据将被发送到第三方服务器上”。同样，黑客还可能通过智能家电从WiFi网络中获得用户密码，甚至掌握有关电器使用情况的数据，推算出用户的活动时间，从而判断用户的生活规律等隐私。“最危险的情况就包括黑客掌握了这些私人信息，设备所有者的合作伙伴能跟踪用户在哪里和与谁共度时光，盗贼可以确认用户什么时候不在家”。

埃森哲公司在俄分部信息安全业务部经理马拉特·崔赫米斯特罗夫表示，用于收集信息最常见的设备是智能手机、监视设备、家用电器等，它们收集的数据范围很广：照片、视频和音频材料、电子邮件和设备状态等。如果对某人发动针对性的网络攻击，几乎可以在线观察他的生活，收集到的数据随后可用于各种目的——勒索、破坏商业活动或个人利益等。对于受害者来说，这样的数据收集通常不会被察觉，他甚至不知道自己正在被追踪。

可能造成更严重后果

这样的担忧并非杞人忧天。俄罗斯网络安全公司卡巴斯基曾发布报告称，相比传统的电脑和手机，物联网设备的低成本特性决定了其针对黑客入侵的防备要宽松得多，这给了不法分子发动网络攻击的机会。根据相关统计，每年物联网设备遭到的网络攻击数以亿计，而且还在飞速增加。美国联邦调查局2020年曾警告称，美国已发生多起犯罪分子利用黑客手段控制受害人家中的智能设备向执法部门报假警的情况，甚至在警员抵达受害人家门口时，犯罪分子还嚣张地通过智能门铃观看现场视频，并借助扬声器与警方对话。在某些极端情况下，还出现过度紧张的警方破门而入、射杀毫不知情的受害人的惨剧。

智能设备存在的网络安全隐患还不只限于个人隐私方面。美国加州理工学院的研究报告称，随着越来越多的物联网设备投入使用，它们很可能成为“僵尸网络”的受害者，在大规模网络攻击中成为“帮凶”。传统的僵尸网络是指成千上万甚至数百万台电脑被犯罪分子通过技术手段远程控制后，就如同只能听从主人指令的“僵尸”，犯罪分子可以进而发起分布式拒绝服务攻击、大规模垃圾邮件活动或其他类型的网络攻击。由于物联网设备的安全防护等级比电脑低得多，而数量却多很多，因而成为近年来犯罪分子建立僵尸网络的首选。2016年，这种利用物联网设备发动的僵尸网络攻击就曾造成美国和欧洲的大范围网络中断。2018年，美国首次发现主要针对智能电视的僵尸网络攻击。

这些被控制的智能设备还可能造成更严重的后果。例如犯罪分子通过僵尸网络同时集中开启某个地区的空调、冰箱等大功率耗电设备，让电网的电力需求突然猛增，进而导致局部大面积供电中断甚至是大规模停电。

应设置复杂密码

如何应对智能家电设备的安全漏洞呢？俄欧米茄公司总经理阿列克谢·雷巴科夫表示，用户自身网络安全意识薄弱，最容易遭到黑客入侵。例如连入不带密码的蓝牙连接时，获得访问权限的攻击者可以控制所有连接的设备。实际上，很多智能家电自身带有安全功能，但用户往往并不知道，或为使用方便而将其禁用。最典型的做法就是不更改制造商默认分配的密码等。

为了保护自己免受智能家电监视，雷巴科夫建议人们通过设置复杂的密码来保护设备和WiFi，并避免使用那些所有用户、设备或程序均可访问的家电。使用智能摄像头时应尽量选购带有加密功能的产品；使用时应启用双重认证，也就是登录时需要密码和验证码的双重认证。此外，应尽量避免用同一个账号和密码登录多个平台，密码设置上也应尽量复杂。费多罗夫称，避免成为黑客或全球数据泄露受害者的最好方法是仅使用“离不开的那些智能技术”，并定期更新设备软件。在涉及隐私的场合中，应关闭家电内置的麦克风，并可通过物理方法断开网络，例如将智能咖啡机断电，将智能手表放在屏蔽盒中，并且可以用超声波干扰器来削弱扬声器。

海外传真

印度拟公布“可信赖电信商”清单

本报讯 据印度《铸币报》报道，印度政府日前要求电信商只能采购可信赖的电信设备后，预计6月将公布可信赖的电信设备制造商名单。

《印度斯坦时报》援引一名未透露姓名的印度官员话表示，印度电信部门正在制定列入“可信赖”来源制造商的标准，如果中国企业符合标准，也可被列入可信赖电信设备供应商名单。

报道指出，印度相关部门共同拟定可信赖电信设备制造商标准。据一名不愿公开姓名的印度官员透露，印度目前对采购电信设备没有任何形式的禁令，多数电信服务供应商都是以最低投标价来采购电信设备，但印度政府担心一些电信设备将对所谓印度的国家安全构成威胁。

因此，除电信设备商外，印度政府也将对英特尔、高通等电信设备芯片与半导体制造供应商进行审查，以决定要把哪些供应与制造商列入可信赖的采购名单。

报道指出，印度政府计划在今年底或明年初推出第5代移动通讯标准(5G)服务，如果禁止中国供应商参与，印度可能只剩下诺基亚、爱立信和三星等公司的设备可以采购，这将影响印度电信营运商的成本。 (胡博峰)

意大利逾270万企业和个人或将面临银行违约风险

本报讯 据欧联通讯社报道，意大利独立银行联合会日前表示，根据欧洲银行业管理局(Eba)新标准，到2021年6月底，大约有3000亿欧元企业和个人银行贷款将无法延期，可能有270万企业和个人面临银行违约风险。

据报道，这些到期的贷款涉及130万家企业和140万个人。由于欧洲的坏账规定于去年1月生效，政府规定将贷款暂停期延长到2021年6月，并在2021年预算法中纳入了一项规定。但是，进一步推迟欧洲银行业管理局准则的实施将不再可能，也不足以避免270万企业和个人陷入财务困境的风险。

意大利银行业协会主席帕图利(Antonio Patuelli)日前在与欧盟经济事务专员加里蒂尼(Paolo Gentiloni)会晤后，呼吁欧盟延长针对意大利企业和个人的紧急财政措施，因为新冠大流行正在加剧。帕图利说，如果3000亿欧元银行贷款到6月底无法延期，而疫情对经济影响依然存在，那么冻结这些贷款将会造成灾难性后果。

欧洲银行业管理局这些限制自2020年1月起生效，包括新的、严格的规则及对不良贷款的管理。据估计，目前，意大利利率处于暂停状态无法结清欠款的主体中，有很大一部分已被银行机构纳入违约。

2021年3月早些时候，意大利国家统计局发布报告指出，2020年，意大利的国民生产总值GDP下降8.9%；而赤字与国民生产总值的比率在2019年的1.6%之后，达到9.5%。 (黄 鑫)

美国医院存在刻意阻挠消费者获取收费信息问题

本报讯 据美国《华尔街日报》报道，美医院存在刻意阻挠消费者获取收费信息的问题，其原因是院方试图在不违反美国政府相关规定的同时，避免其收费信息完全透明化。

报道称，经过对3100家医疗机构网站调查后发现，数百家美国医院通过在其网站内嵌入特殊编码，迫使消费者必须跳转多个网页才能获取收费信息或价目表。

报道援引华盛顿大学人机互动领域的副教授奇拉格·沙阿的话说，虽然从技术角度看这些费用信息都是公开的，但很明显院方刻意对信息进行了处理，使其难以被搜索到。

美国医疗行业长期存在收费信息不透明的问题。美政府规定，自今年1月1日起，医院必须如实披露收费信息，确保公开透明，以便更好保护公众利益。

(夏 林)

本报社址：北京市亦庄地盛西路6号中改传媒大厦 邮政编码100176 值班电话(010)56805051 广告发行部(010)56805116 广告经营许可证：京大工商广登字20180001号 零售价2.00元 本报照排 经济日报印刷厂印刷