教育部人文社会科学研究规划基金项目资助【17YJA870005】

物联网场景下个人隐私信息泄露的治理体系构建研究

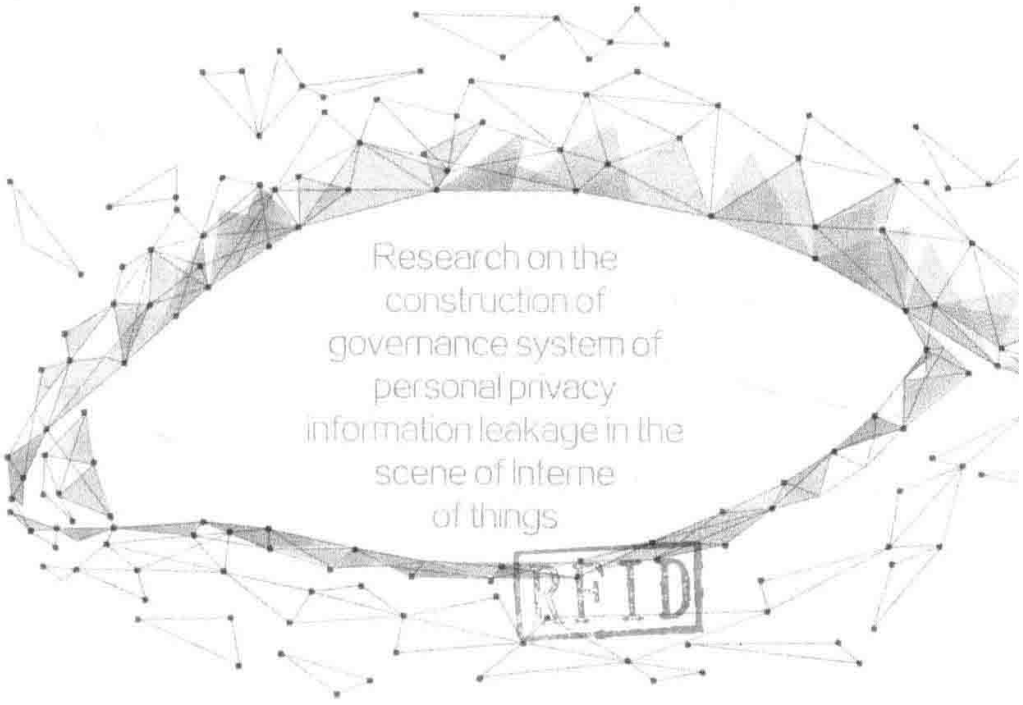
董新平　叶彩鸿　蒋怡　吴刚　著

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

教育部人文社会科学研究规划基金项目资助【17YJA870005】

物联网场景下个人隐私信息泄露的治理体系构建研究

董新平　叶彩鸿　蒋怡　吴刚　著



ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

图书在版编目（CIP）数据

物联网场景下个人隐私信息泄露的治理体系构建研究 / 董新平等著. — 杭州 ： 浙江大学出版社，2020.12
ISBN 978-7-308-20867-3

Ⅰ. ①物… Ⅱ. ①董… Ⅲ. ①物联网－电子传感器－信息安全－研究 Ⅳ. ①TP212.4②G203

中国版本图书馆CIP数据核字（2020）第241381号

物联网场景下个人隐私信息泄露的治理体系构建研究

董新平　等著

责任编辑　赵　静
责任校对　董雯兰
封面设计　杭州林智广告有限公司
出版发行　浙江大学出版社
（杭州市天目山路148号　　邮政编码　310007）
（网址：http：//www.zjupress.com）
排　　版　杭州林智广告有限公司
印　　刷　广东虎彩云印刷有限公司绍兴分公司
开　　本　710mm×1000mm　1/16
印　　张　10.5
字　　数　177千
版 印 次　2020年12月第1版　2020年12月第1次印刷
书　　号　ISBN 978-7-308-20867-3
定　　价　42.00元

前 言

在隐私发展的历史进程中，科学技术与隐私相伴发展，并且科技进步极大地影响了隐私演化的进程。19世纪90年代，当路易斯·布兰代斯（Louis Brandeis）和塞缪尔·沃伦（Samuel Warren）发表具有里程碑意义的经典论著《隐私权》时，世界为之震惊。两位杰出的法学家将隐私定义为“独处的权利”，倡导在应用摄影等技术时应尊重个人隐私。之后，电话的发明开创了远程电子通信时代，引发了关于政府窃听电话内容是否构成侵犯个人隐私的激烈辩论。此后，信息技术不断发展进步，特别是20世纪90年代互联网的兴起带来了新的隐私问题，隐私偷窥者不用入侵个体物理空间也可以通过网络“偷窃”其隐私，这极大地冲击了原有的“保持独处”隐私理论。人们开始观察到隐私内涵外延的深刻变化：物理交互不再是个人信息传输所必需的途径，数据可以在一个全球联网的计算机网络世界自由流动，个人隐私泄露不再一定要侵入个人物理空间，没有个人物理交互的网络虚拟空间也能造成隐私泄露和侵犯。

电话的发明标志着通信技术和文化的一个历史性的进步，但是法律系统花了几十年的时间来适应隐私理论的新变化。物联网技术的出现又将隐私隐患问题推到了一个新的历史高度。传统的互联网将人与人之间的信息交换联系在一起，物联网则将机器、人与嵌入式传感器结合起来，使它们能够通过网络进行自由交换、自主通信。数以亿计的传感器设备投入使用后，一个全民“被监视”的“裸奔时代”正向我们走来。物联网这种特殊的“自动采集信息、自动传输与存储信息、自动分析处理信息、智能化应用信息”特征，造成了个人隐私泄露危害可能大大超出人们的预期，甚至可能带来难以想象的灾难性的后果。法国学者马尔克·杜甘（Marc Dugain）甚至认为物联网的全面应用可能使人

类重返赤裸裸的“原始人时代”[①]。呼吸计（Breathometer）若用于性格和行为推断，就业、保险、信贷等方面的商业规则和商业文明将被完全颠覆，婚姻择偶、家庭情感、朋友友情等道德伦理将面临洗牌的风险。

从现有研究成果看，保护个人隐私是社会进步的重要表现，因为它支持自由、财产权、知情同意、个性发展、幸福、权力平等，适当分离社会多个区域和社会组织权利，同时有助于防止歧视诽谤，每个国家都有必要建立专业的个人隐私信息保护体系。反之，若忽视了个人隐私保护体系建设，则可能带来安全、伦理问题，甚至灾难。

目前，美国一些立法部门可能会采取应对行动，禁止利用从多种物联网设备中提取的数据用于商业服务，禁止追踪和测量我们隐私敏感的两个环境——身体和家庭。虽然在就业、保险和信贷决策中，健身、健康、家用电器和家庭习惯数据可能具有经济价值，但公众有可能对这种敏感个人信息的利用反应强烈。美国正在考虑在新的或修改的法规中禁止其在某些敏感产品中的应用，也在限制汽车和驾驶数据用于就业、信贷和住房决定，以及在汽车保险、健康保险范围内的应用。

从案例和实证分析可以看出，“隐私泄露的管理过程和隐私深度利用”“隐私制度建设”是用户隐私泄露容忍度最低的领域，国家应该重点加强这方面的规则建设。物联网场景下个人隐私泄露治理需要从用户需求入手，加强隐私泄露对象监管，关注空间隐私与活动隐私，关注身体与健康隐私等重点领域，提高物联网产品制造者责任意识，加强民众物联网隐私科普，加强政府立法和监管，构建符合我国社会文明的治理体系。

本书各章撰写分工如下：第一章、第二章由董新平（浙大宁波理工学院）、吴刚（浙江科技学院）研究、执笔，第三章、第四章由叶彩鸿（宁波大学）研究、执笔，第五章、第六章由董新平、蒋怡（浙大宁波理工学院）研究、执笔。全书由董新平确定研究思路和提纲，并统稿。

董新平

2020年8月

① [法]马尔克·杜甘. 赤裸裸的人——大数据，隐私与窥视 [M]. 杜燕，译. 上海：上海科学技术出版社，2017：54.

目 录

第一章

物联网及其他新技术带来的隐私挑战

第一节 新技术带来的隐私挑战

一、技术对隐私的影响

在隐私发展的历史进程中，科学技术与隐私相伴发展，并且科技进步极大地影响了隐私演化的进程。19世纪90年代，当路易斯·布兰代斯（Louis Brandeis）和塞缪尔·沃伦（Samuel Warren）发表具有里程碑意义的经典论著《隐私权》时，世界为之震惊。同时，《隐私权》也激发了人们对隐私概念的关注，引出了一系列隐私理论。那时，摄影设备还是刚发明的新技术产品，摄影设备的摄像功能引起了人们对隐私问题的担忧，一些人抨击摄影设备可能会侵犯人们的隐私。在那个特定的时代背景下，路易斯·布兰代斯和塞缪尔·沃伦两位杰出的法学家将隐私定义为“独处的权利”，倡导在应用摄影等技术时应尊重个人隐私。①

之后，电话的发明开创了远程电子通信时代，引发了关于政府窃听电话内容是否构成侵犯个人隐私的激烈辩论。现代信息技术创新的另一个时代开始于20世纪50年代，那时计算机和磁带技术的出现大大提高了信息存储和运算能力。此后，信息技术不断发展进步，特别是20世纪90年代互联网的兴起带来了新的隐私问题，隐私偷窥者不用入侵个体物理空间也可以通过网络“偷窃”其隐私，这极大地冲击了原有的“保持独处”隐私理论。

随着互联网时代的到来，人们开始观察到隐私内涵外延的深刻变化：物理交互不再是个人信息传输所必需的途径，数据可以在一个全球联网的计算机网络世界自由流动。由于这个网络系统是虚拟的、数字化的，个人隐私泄露不再一定要侵入个人物理空间，没有个人物理交互的网络虚拟空间也能造成隐私泄露和侵犯。数字技术的创新促进了互联网的发展，数字技术与网络技术、光纤通信技术结合使互联网存储、汇总和传输数据的能力急剧增长，促进了跨越国

① CHANG C H. New Technology, New Privacy Facing Information Privacy Challenges in an Age of Emerging Information Technology. American University, 2016: 9-81.

界的海量数据即时传输、交互。此外，无线互联网服务和移动设备的革命再次极大地改变了全球通信格局，方便了人们随时随地连接、沟通，也打破了传统隐私理论的空间边界。

电话的发明标志着通信技术和文化的一个历史性的进步，但是法律系统花了几十年的时间来适应隐私理论的新变化。事实上，法律系统跟不上科学技术变革的步伐也许是可以容忍的，因为使用电话作为侵犯隐私的工具突破了原有的隐私法框架。现在我们正处在一场前所未有的技术革命浪潮中，广泛的数据、互联网技术的力量并不只是给人类带来福祉，也可能给人类带来新的隐患，甚至灾难。如果不建立相应的隐私理论框架和法律体系，个人自由很容易受到隐私控制，人类的进步和发展将受到冲击。①

物联网技术的出现又将隐私隐患问题推到了一个新的历史高度。物联网利用互联网可形成一个庞大的智能对象网络。传统的互联网将人与人之间的信息交换联系在一起，物联网则将机器、人与嵌入式传感器结合起来，使它们能够通过网络进行自由交换、自主通信。保守的预测数据表明，到2020年将有超过2000亿个连接的传感器设备投入使用，一个全民“监视”的时代正向我们走来。物联网的出现使个人隐私信息的采集、生成、传播和处理分析不一定需要人工的参与，而是自动采集、自动生成、高效快捷传播和智能化自动化处理。物联网这种特殊的“自动采集信息、自动传输与存储信息、自动分析处理信息、智能化应用信息”特征，使得个人隐私泄露危害可能大大超出人们的预期，甚至可能带来难以想象的灾难性后果。法国学者马尔克·杜甘（Marc Dugain）甚至认为物联网的全面应用可能使人类重返赤裸裸的“原始人时代”。呼吸计（Breathometer）若用于性格和行为推断，就业、保险、信贷等方面的商业规则和商业文明将被完全颠覆，婚姻择偶、家庭情感、朋友友情等道德伦理将面临洗牌的风险。

二、新兴技术引发的隐私问题的共同特征

新兴技术的出现引发了大量的隐私问题，也对传统隐私概念的内涵、外延

① LINDA J. GOMBERG. The Case for Privacy: A History of Privacy in the United States as Seen through a Psychological Lens and Defined by Case law and the Impact of Social Media. Fielding Graduate University，2012：76-91.

带来了冲击。因此，探讨新兴技术如何改变隐私作用机制，以及由新兴技术引发的隐私问题的共同特征非常有必要。互联网和电子移动设备的广泛使用给个人带来了极大的便利，人们有强烈的电子移动设备使用动力和意愿。企业则发现利用个人数据挖掘技术可以轻易地获取消费者的个人行为数据（如购物行为和个人偏好），于是大量的企业急急忙忙使用数据挖掘技术工具“偷窃”个人信息及个人行为数据，丝毫不顾及用户的意见，甚至在用户毫不知情的情况下滥用其个人信息及个人行为数据。

用户在线信息行为保护是隐私领域的一个重要议题，涉及用户网络信息行为是否可以被跟踪、个人数据在移动设备上存储时是否应该得到深度保护、用户的网络行为数据是否可以和其他行为数据进行结合聚类分析等。[①]如DED和其他在线数据收集设备可以一键自动云抓取用户网络数据，将消费者行为暴露于大庭广众之下，这种技术应用用户知道吗？用户接受吗？一些企业通过技术工具获得用户的地理位置数据，并分析用户的活动范围和规律，基于抓取到的物理位置数据来发出针对性的个人广告。同时，一些企业使用基于网站的“cookies”技术来数字化地跟踪用户活动，当用户访问一些网站时，从用户的计算机数据文件中随意获取用户信息。如一种更先进的深度分组检查技术（DPI），能使互联网服务提供商（ISP）轻松收集消费者与消费者之间的所有互联网交互信息，分析他们的网络流量，并编译“Web使用记录”，以开发特定客户或客户组的专用广告。这种以意想不到的方式使用用户网络数据的危险行为并非网络世界所独有，如杂货店正准备推出一种新的高科技设备，即智能货架，根据收集到的消费者购物习惯信息，并通过检测传感器进行实时的现场性购物推荐。这明显超出了传统的隐私认知范畴，个人隐私被侵犯、放大和蔓延的问题正变得越来越严重，而不再局限于那些选择使用新技术的社会成员。

许多新的个人信息攫取技术正在投入使用，不同的新技术也可能会引发不同的隐私问题。人们现在关心的基本问题是:新信息技术对个人隐私的挑战有哪些?新技术环境下个人隐私的性质是否发生了变化，还是由于技术的变化而产生了一种新的隐私类型?只有正确认识到新信息技术时代下的隐私威胁，我们

① MICHAEL CORLISS. The Use of Information: How New Technology is Changing Discussions of Privacy. Georgetown University, 2010: 36-56.

才能更好地评估现有法律是否足以覆盖现有隐私威胁，才能有针对性地开发新技术以应对现有威胁隐私的挑战。

由于互联网的广泛使用，一些能反映新兴隐私特征的方面已经呈现出来。一是更详细和深入的个人网络喜好和兴趣活动，如互联网搜索词和网站访问的历史记录。二是廉价的数据存储媒体和更快的信息聚合和传输载体，如公共网络服务器或云存储器。当个人信息存储在公共网络服务器或云中，或者公共信息和私人信息交互融合时，公共信息和私有信息之间的界限就变得模糊了，这直接导致传统的隐私内涵失效。

与传统信息流相比，互联网信息有如下特征：一是信息处理和传播速度更快，数量更多；二是持续性久，在线发布的互联网信息具有“持久性”，不仅可以被轻易地复制、存档，而且可以以数字文本形式低成本地保存；三是快速有效地搜索，任何人都可以“快速有效地”搜索一个网络平台、网站、数据库，通过关键字、主题词搜索网络信息资源；四是受众对象的不确定性，当我们在网上分享帖子或发布信息时，我们无法预知发布的信息是否会被特定的对象看到，而传统的信息流对象则是确定的。

互联网信息流与传统信息流的差异，造就了网络隐私与线下隐私的差异。如网络隐私没有传统隐私的国别概念;由于互联网环境下具有更大的存储容量，数据保留时间长、数量多，也更容易获得，这使得网络隐私更容易泄露和扩散。

新兴技术特别是互联网技术促进了个人信息的收集、获取和使用，而不受地点和时间的限制。但是，这种便利的个人信息收集、获取和使用却带来了隐私保护的困难。并且，用户对于个人信息是否被收集，以及这些个人信息可能被如何使用只会变得更加难以知晓。现有的隐私法律和政策是在这样的假设下制定的，即一个人应该能够完全控制自己的个人信息，并能决定如何使用这些个人信息。但是，如果新兴技术的出现，使得个人不太可能被告知和控制他们自己的个人信息，那么这个假设将不再成立，隐私的法律和政策也将面临挑战。

三、大数据和移动技术引起的隐私问题的进一步放大

大数据（big data）是指无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的大量数据的聚合。“大数据”的“大”有两层含义：一是可以处理

数据的数量多、种类多；二是这些数据的作用很大、贡献大，应用这些数据进行处理能产生许多科学推断并服务人类。但是，大数据越来越多地被用来描述复杂的计算能力过程、最新的机器学习、人工智能以及大规模和高度复杂的数据聚合，这些应用也会带来新的隐私问题。

其中，“Google预测流感趋势”就是大数据应用的一个典型案例，它解释了“大数据”是如何利用新技术预测公共卫生领域的舆情。其原理在于，Google通过观察人们在谷歌搜索引擎中键入的流感症状来预判流感暴发的规模、时间、严重程度等。“Google预测流感趋势”这个项目确实证明Google大数据应用能够比疾病控制和预防中心提前一到两个星期预测到流感的暴发。但是，由于没有遵守传统的隐私信息通知、选择以及透明度原则，“Google预测流感趋势”这个项目被认为是以破坏个人隐私信息和背叛公众的信任为代价的。确实，“Google预测流感趋势”这个项目在实施时没有向人们提供隐私选择和告知过程，没有让人们自己决定是否将敏感数据应用于公共卫生管理。这个项目尽管解决了一个传统难题，但也提出了一些新问题。

从技术实现原理角度看，大数据并不仅仅是根据历史数据分析消费者偏好，它也可以用来影响消费者的网络行为。在线社交网络Facebook在2014年6月曾发布了一项实验成果，该成果表明Facebook新闻订阅可以影响网络情绪。一位Facebook的研究人员表示，这个实验的目的是“调查人们普遍担心的问题，即看到朋友发布积极的内容是否会导致人们感觉积极心理”。同时，研究人员也担心暴露在朋友圈的消极情绪是否会导致人们避免或减少使用Facebook等社交媒体工具。社交网络Facebook的试验表明，大数据技术不仅可以预测网络舆情，也能影响网络社会心理，这实在是大大超出了研究者的预期。①

大数据应用产生了明显的隐私问题，但是关键是任何人都不可能被排除在错综复杂的数字和互联网世界之外。一个人即使不使用任何互联网和移动设备，但传统的信息控制方法对个人隐私信息保护仍不会有效，他仍然会被困在无法逃脱的数字网络之中，其他人仍然能够追踪他的个人数据或行为活动。

我们必须面对这样一个事实：在这个科技发达的时代，人们没有真正有效

① LARS WEISE. The Politics of Personal Information Privacy for the Facebook Age–towards an Articulation and Assemblage Theory of PIP. University of Minnesota，2014：65–102.