

城市智慧创新国际联合研究丛书

丛书主编：关成华

北京师范大学城市绿色发展科技战略研究北京市重点实验室

TRUST :: DATA

A New Framework for Identity and Data Sharing

信任与数据

身份与数据共享的创新框架

[美] 托马斯·哈乔诺 大卫·舍瑞尔 阿莱克斯·彭特兰 编著
陈浩 译



中国财经出版传媒集团



经济科学出版社
Economic Science Press

城市智慧创新国际联合研究丛书

丛书主编：关成华

北京师范大学城市绿色发展科技战略研究北京市重点实验室

TRUST :: DATA

A New Framework for Identity and Data Sharing

信任与数据

身份与数据共享的创新框架

[美] 托马斯·哈乔诺 大卫·舍瑞尔 阿莱克斯·彭特兰 编著
陈浩 译

许崇清
陈嘉庚
李光前
陈延谦

何凤翔
李光前
陈延谦
陈延谦

中国财经出版传媒集团



经济科学出版社
Economic Science Press

图书在版编目 (CIP) 数据

信任与数据：身份与数据共享的创新框架/(美) 托马斯·哈乔诺, (美) 大卫·舍瑞尔, (美) 阿莱克斯·彭特兰编著; 陈浩译. —北京: 经济科学出版社, 2018. 10

书名原文: Trust;: Data: A New Framework for Identity and Data Sharing

ISBN 978 - 7 - 5141 - 9866 - 9

I. ①信… II. ①托…②大…③阿…④陈… III. ①移动通信 - 通信技术 - 应用 - 金融 - 商业服务 - 研究
IV. ①F830 - 39

中国版本图书馆 CIP 数据核字 (2018) 第 239922 号
图字 01 - 2018 - 6529

责任编辑: 周秀霞

责任校对: 曹育伟

责任印制: 李 鹏

信任与数据:

身份与数据共享的创新框架

[美] 托马斯·哈乔诺

大卫·舍瑞尔 编著

阿莱克斯·彭特兰

陈浩译

经济科学出版社出版、发行 新华书店经销

社址: 北京市海淀区阜成路甲 28 号 邮编: 100142

总编部电话: 010 - 88191217 发行部电话: 010 - 88191522

网址: [www. esp. com. cn](http://www.esp.com.cn)

电子邮件: [esp@ esp. com. cn](mailto:esp@esp.com.cn)

天猫网店: 经济科学出版社旗舰店

网址: [http://jjkxcbs. tmall. com](http://jjkxcbs.tmall.com)

北京季蜂印刷有限公司印装

710 × 1000 16 开 14.5 印张 210000 字

2018 年 11 月第 1 版 2018 年 11 月第 1 次印刷

ISBN 978 - 7 - 5141 - 9866 - 9 定价: 48.00 元

(图书出现印装问题, 本社负责调换。电话: 010 - 88191510)

(版权所有 侵权必究 打击盗版 举报热线: 010 - 88191661)

QQ: 2242791300 营销中心电话: 010 - 88191537

电子邮箱: [dbts@ esp. com. cn](mailto:dbts@esp.com.cn))

信任与数据：
身份与数据共享的创新框架

Trust:: Data
A New Framework for Identity and Data Sharing

VISIONARY FUTURE

[www. VisionaryFuture. com](http://www.VisionaryFuture.com)

© 2016 Visionary Future LLC. 版权所有

本书部分内容先前已发表过，经作者同意转载于此

编著者

[美] 托马斯·哈乔诺 大卫·舍瑞尔 阿莱克斯·彭特兰

致谢

感谢我们的孩子，他们激励着
我们创造更加美好的明天

城市智慧创新国际联合研究丛书

主 编 关成华

学 术 顾 问 阿莱克斯·彭特兰 李晓西 郭 为
韩国义 张建平

编 委 陈 浩 涂 勤 张江雪 宋 涛
郑艳婷 肖 尧 施发启 赵 峥
崔 琦 彭玉珏 张佑辉

本书参与人员 宋 涛 郑艳婷 肖 尧 崔 琦
魏 杨 彭 桥 贺 玲 王琳娟
马丹丹 陈美佳 许婉婷

单 位 北京师范大学
城市绿色发展科技战略研究北京市重点实验室

目录

导言 可信任数据	1
第1章 迈向可信数据的互联网	11
第2章 核心身份：未来交易系统的核心身份	33
第3章 OPAL / ENIGMA	51
第4章 重塑社会契约：数据新政	67
第5章 去中心化个人数据市场的兴起	83
第6章 手机数据的人道主义使用方式	93
第7章 可信任数据的生活实验室	103
附录 A 个人数据：一个新的资产类别的出现	115
附录 B 一个具有重要意义的世界：动员数据革命促进可持续发展	155
参考文献及注释	187
作者简介	215

导言 可信任数据

托马斯·哈乔诺

大卫·舍瑞尔

阿莱克斯·彭特兰

社会的神经系统^①

我们和麻省理工学院的同事们正在尝试创造未来。在我们看来仅仅评估、分析世界的现状，预测变化趋势是不够的。我们试图创造新的工具、框架，帮助人们达成共识，创造美好明天。

当前在数据、个人隐私和信息安全领域，依然存在许多问题，但难以找到有效的解决方案。各国政府日渐意识到目前高成本与风险的状况，并急于改善。

本书将介绍对技术和方法的新思考，包括如何更好地管理身份（identity）、保护个人信息、改善信息的应用方式及保护关键数据免受攻击。我们将探索“数据新政”的意义及人们赋予个人信息的价值，包括在法律和政策方面的含义。

为此，我们在世界多处，包括意大利的特伦托、哥伦比亚的波哥大等地，建立了“生活实验室”（Living Labs），用以测试上述信息管理相关技术的实施效果。

政府、能源和公共卫生数据系统的信任构建

构建可信任的数据系统，并理解其构建的动力和框架及数据系统本身所蕴含的信任含义，是大有裨益的。维系一个健康、安全和高效的社会系统是一项挑战，其甚至可以追溯到19世纪。当时的社会经历了工业革命的剧烈变革，刺激了城市的快速增长，也引发了严重的社会环境

^① 本部分的早期版本出现在2012年1月的IEEE Computer期刊上，作者是阿莱克斯·彭特兰。

问题。当时的解决方案是通过建立中心化的健康、安全、教育网络系统，提供清洁水、安全食品、垃圾清除、能源供给和便利的交通等系列服务。

这些历经百年的解决方案日渐陈旧。而当代社会依然缺乏整体性设计，致使社会无法利用新的数字反馈技术动态的反映社会系统的变化。

我们需要深入反思当前的做法。不是仅按功能将社会系统划分为水系统、食物系统、废物回收系统、交通系统、教育系统、能源系统等多个单一系统进行孤立分析，而应采用综合性的分析方法。不是仅聚焦于如何使用和分配系统，而是应该通过设计一个复杂的连接网络，去构建动态的、网络化的自我调节系统。简而言之，为确保未来社会的可持续发展，我们必须利用不断发展的技术为人类社会创造一个智慧型的“神经系统”（Nervous System），以维持国家政府、能源和公共卫生系统的稳定发展。

我们的核心思想是重塑一个实时的、积极动态的社会系统：通过情态感知，将观测数据与动态的需求—反应模型相结合，并通过预测更新系统。幸运的是，许多感知器和相应的数据更新系统已经就位。然而，我们当前所缺乏的是建立在可信数据架构之上的动态交互模型，用于保障数据的安全、稳定和效率。

人是所有这些系统的核心，个人行为的交互正以几何级数增长的模式产生了大量数据，所以我们必须通过仔细观察个体行为，构建相应的模型，以描述人的需求和行为反应。

梅格莱娜·库内娃在2007年至2010年期间担任了欧盟委员会消费者权益保护事务专员，强调了个人行为数据的重要性，并将数据形容为“互联网的新石油和数字世界的新货币”^[1]。

随着行为感知数据的快速增长，未来系统的架构必须能够充分保障所有潜在参与者的个人隐私与公平对待。正如美国联邦贸易委员会主席乔恩·莱博维茨所说：“隐私和安全保护从一开始就必须嵌入到公司的程序、系统和技术中，使之成为公司商务模式的有机组成部分。”^[2]

阿莱克斯·彭特兰认识到利用无处不在的移动感知来重塑社会基础设施需要全体公民、政府和企业的共同支持，于2007年在世界经济论坛（WEF）提出了建立“数据新政”（A New Deal on Data）^[3]的构想，由此开启长达多年的由IT、无线、基础设施和金融公司的领导人以及各种国际监管组织和非政府组织负责人共同参与的对话（就“数据新政”，第4章中将作详细解读）。

这次讨论催生了次年的“重新思考个人数据”（Rethinking Personal Data）项目（www.weforum.org/issues/rethinking-personal-data），并于2011年出版了《个人数据：一个新的资产类别的出现》一书，对“数据新政”的认识渐趋一致，提供了对未来路径的深刻见解^[4]（见附录A）。

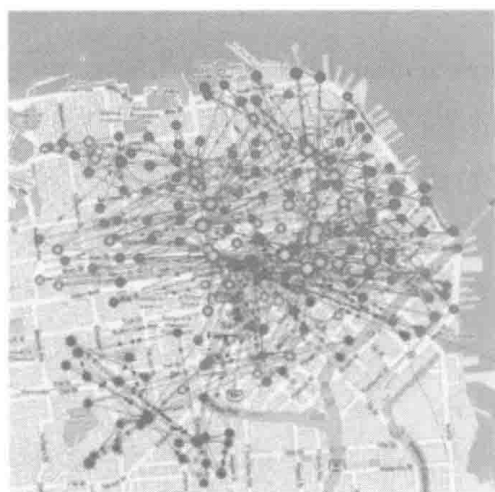
无处不在的感知

由移动电话产生的位置数据是一个最好的例子。这些数据在过去十年来非常普遍，对社会极具价值，但非常敏感。

全世界现在有超过50亿的手机用户，且按每天数百万新用户的速率持续增长。庞大的手机用户通过语音联系在一起，这在人类历史上还是首次。更重要的是，手机是位置感知平台，通过连接无线网络，感知人们日常生活、工作以及交通位置信息。我们可以通过手机这种移动无线基础设施进行“现实挖掘”，来了解人类的行为模式，监测环境，并规划社会的发展。目前这种功用尚未充分发掘，但是研究人员已经利用感知功能，来测度城市人口变迁，绘制在自然灾害和紧急情况下的人口流动分布，追踪疾病的暴发，识别社会服务欠缺的社区，以及监管交通拥堵^[3]。

图1由A、B两图组成。其中，图1A基于手机的GPS数据揭示了城市内的移动模式，并且对餐厅、娱乐场所等地方的常见移动模式进行

了颜色编码。图 1B 通过甄别这些移动模式揭示出不同行为模式的子群体。对行为模式分类通常比标准的人口统计学能更准确地预测人们患某些疾病（如糖尿病）的风险、消费偏好、财务风险和政治观点。同时，在促进公共卫生、改善城市规划、加强救灾能力和发展公共教育等方面也显示出了巨大潜力^[4]。



© 2008 Sense Networks, Inc.

A. 城市内移动模式



© 2008 Sense Networks, Inc.

B. 部分群体的不同行为模式

图 1 基于手机 GPS 数据的城市内移动模式

数据所有权和隐私

无处不在的感知系统所带来的最大挑战是用户数据的所有权和隐私之间的矛盾^[3]。网络数据分析技术的发展既要为数据所有者创造价值，同时又必须保护用户的隐私。

这些数据不能被私人公司独自掌握，否则将不能对公共利益有所增进。同时，这些数据也不能被政府独揽，如果这样，将会降低数据的透明度，损害公共利益。同样的，我们应该强制使用匿名数据，然后才可汇总结果。强大的协作和数据共享模式必须既能保护消费者的隐私又能信任与数据

保护企业的竞争利益。

目前，私人机构收集了绝大多数个人数据，比如位置模式、金融交易、电话和互联网通信等等，私人机构由此将成为数据隐私和所有权谈判中的关键角色。人们希望有相应的政府监管和市场机制来鼓励数据所有者分享他们收集到的数据，为个人和整个社会服务。

数据新政 (New Deal on Data)

就像金融市场和商品市场一样，创建信息市场的第一步是定义所有权。这就是为什么世界经济论坛报告的副标题把个人数据称为“新资产”^[4]。要确定“拥有自己的数据”含义，最简单的方法是根据英美法系关于所有权、使用权和处置权的定义进行类推：

- 你有权拥有你自己的数据。无论什么样的组织或个人收集你的数据，这些数据都属于你，你可以随时访问自己的数据。数据收集者扮演类似于银行的角色，代表他们的“客户”管理数据。

- 你有权控制自己数据的使用。数据使用条款必须具有可选性，而且必须以明确的语言加以解释。如果你对公司使用你数据的方式不满意，可以把数据删除，就像你关闭银行账户一样，因为该银行没有提供令人满意的服务。

- 你有权处置或发布自身的数据。你也可以销毁个人数据或将其重新部署到别处。

我们将在第4章对这些概念进行扩展，在这里只作简单扼要的说明：

个人数据的所有权必须与公司和政府的需求相平衡，以便它们使用某些数据（如账户活动、账单信息等）进行日常工作。总之，“数据新政”的主要目的是让人们对自己的个人数据拥有所有权、使用权和处置权。

执行数据新政

行使个人数据所有权不是简单地认证个人的身份，它还要验证个人、机构甚至设备是否有权访问和使用个人数据。随着越来越多的商业、金融和政府服务机构收集和使用个人数据，确保全球身份认证和声明的基础设施的整体性与协作性将会变得至关重要。

由于没有一个权威机构可以对所有的交易、故障和攻击进行微观管理，所以像互联网这样的全球性基础设施必须采取分布式部署并以用户为中心，以便互联网可以快速创新、有效遏制攻击并实现自我纠正。

“开放身份交换”（OIX）等机构使用的信任网络或信任框架就是分布式架构的一个例子，这种分布式架构不仅为大公司所接受，也得到了许多政府的认可。

个人数据信任网络（Trust Network）是与“开放身份交换”（OIX）的数据生态系统非常类似的一种信任网络，它需要对欺诈和欺骗行为进行持续监视和标记。这不仅需要软件的创新来跟踪和审核网络中的交易活动，还需要相关政策和合同法的建立确保交易活动可以简单、公平和有效的执行并在出错的情况下进行补救。

麻省理工学院连接科学实验室（MIT Connection Science）创建的 OPAL/ENIGMA 项目就是为了开发信任网络的原型，以支持世界经济论坛“重新思考个人数据”项目，并测试了该信任网络在万维网（<http://trust.mit.edu>）运行情况。第 2 章和第 3 章将详细介绍 OPAL/ENIGMA 的组成部分。

随着身份的认证和声明完全自动化，法律和行政流程也应该变得更加高效、透明和负责。简而言之，为了实现高度可靠与革新的身份声明，数字技术不仅应该被用来加快全球基础设施的创新，而且还应该用来消除法律与监管的不确定性、成本和摩擦。这将大大降低交易成本，

产生新形态的流动资产和创新型业务。

可被验证的信任能降低交易风险、提高客户忠诚度，因此其信誉可以被验证的个人数据管理者在未来线上服务和移动服务方面将获得极大的经济利益。

真实世界的网络

由传感器产生的个人数据无处不在。这些数据的性质和所涉及范围对于很多人来说是陌生的，但是可以确定的是在互联网上已经存在大量的个人数据。

这些互联网个人数据主要包括3个方面内容：（1）由用户向社交网站、博客和论坛提供的信息；（2）在线商家或机构的交易、注册数据；（3）网络浏览和点击流历史数据。有些研究人员已经开始去挖掘利用这些互联网个人数据，比如对用户提供的图像和视频的挖掘分析，尽管这些数据是用户有意识产生的，但是与被动采集的传感器数据（如通话记录和电话位置数据）一样，仍然是一个挑战。

网络在一个不受管制的环境中演变，对于个人数据的隐私没有一致的标准。对于这些数据的权利，人们并不清楚，而且因人而异。像位置数据、医疗传感器数据等，由受到严格监管的行业收集，这些数据具有相当明确的所有权规定，并且可以通过把数据新政扩展到现有框架获得更广泛的分享。这种不受管制的真实世界的网络应该受到严格监管。幸运的是，现有的网络公司正面临着要达到监管行业所要求的更高标准的压力。

这种压力正在缓慢地推进个人数据的发展。例如，在世界经济论坛领导的第一轮讨论中创立了“重新思考个人数据项目”，在这之后，谷歌发布了 Google Dashboard ([www. Google. com/dashboard](http://www.Google.com/dashboard))，可以让用户知道有哪些数据是关于他们自己的。在第二轮讨论之后，谷歌成立了一

个由工程师团体组成的“数据解放阵线”（www.dataiberation.org），其使命是“用户应该能够控制他们存储在谷歌任何产品中的数据”，其目标是“使数据更容易进出”。

这些新工具有可能把乔治·奥威尔“全控状态”这种反乌托邦式的愿景变为现实。因此，我们必须思考个人数据量的增长以及在驱动社会系统方面日益广泛的使用，尤其是这些数据的安全性、稳定性和公平性。

现行法律水平远远落后于我们收集和处理相关数据的能力；显然，我们的隐私和数据所有权概念必须适应这些新技术。或许建立相关法律的第一步是让人们拥有自己数据的所有权，保证正在成为全球新货币的数据具有所谓的“公平信息做法”。现在是时候利用我们在金融财富分配和管理方面的丰富经验，以公平有效的方式来建立符合我们愿望的社会制度。第4章和第5章对新数字时代的隐私和法律问题进行了深入的思考。

拟议的数据新政可以确保数据责任和数据所有权，我们已经成功地说服政府、行业和非政府组织领导人采用这一新政。第6章和第7章详述了这里所描述的各种要素如何在“生活实验室”（一种新的社会形式）这种紧密联系的现实世界系统中运行。

如果我们能够成功地应对这些挑战，目前的制度将演变成一种有效的社会神经系统。它将为我们的提供更好的公民服务、更绿色的生活方式和更安全、更健康的人文环境方面，并使投资得到多倍的回报。