国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1363

(05/2020)

X系列：数据网、开放系统通信和安全性

安全应用和服务 (2) – 物联网 (IoT) 安全

物联网(IoT)环境下处理个人可识别信息(PII)的技术框架

ITU-T X.1363 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	**X.1360–X.1369**
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
5G 安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1363 建议书

物联网环境下处理个人可识别信息的技术框架

摘要

物联网（IoT）设备能够收集各类数据，包括个人可识别信息（PII）。因为个人可识别信息数据对于不同类型的服务都有用，所以，该信息可以在多个服务提供商之间共享。

用户根据自己的目的在物联网环境下管理其所拥有的数据（包括个人可识别信息）是有好处的。在物联网环境中与多个服务提供商共同使用数据是复杂的过程，应灵活地兼顾用户使用数据的意图。例如，如果某个物联网服务提供商提供下列功能，用户可认为服务提供商恰当地收集和控制了所收集的数据（包括个人可识别信息）：

– 用户可以配置其自己的个人可识别信息首选项。这些首选项包括允许与其他服务提供商共享的数据列表。

– 应根据个人可识别信息首选项有控制地进行数据收集和共享。未授权的数据不能存储在数据存储器中，也不能与其他服务提供商共享。

– 用户可以检查服务提供商之间共享数据的历史日志。用户还可以检查其数据共享的时间。

ITU-T X.1363建议书规定了在物联网环境下通过一个或多个服务提供商处理个人可识别信息的技术框架。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1363	2020-05-29	17	11.1002/1000/14087

关键词

IoT、个人可识别信息、PII。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1363 建议书

物联网环境下处理个人可识别信息的技术框架

1 范围

本建议书规定了在物联网环境下处理个人可识别信息（PII）的技术框架。

在物联网环境下，某些物联网设备具有收集个人可识别信息数据的能力。由于个人可识别信息数据对于各种类型的服务都有用，因此数据可以在多个服务提供商之间共享。本建议书中规定的技术框架为一个或多个物联网服务提供商收集、共享和使用物联网用户的个人可识别信息数据提供了保护机制。

2 参考文献

下列ITU-T建议书和其他参考文献所包含的条款通过本案文的引用而成为本建议书中的条款。出版时，所显示的版本是有效的。所有的建议书和其他参考文献都需要修订，鼓励使用本建议书的各方应探讨能否使用下列建议书和其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T X.1058] ITU-T X.1058建议书（2017年）| ISO/IEC 29151:2017，信息技术 – 安全技术 – 个人可识别信息保护的实施规程。

[ISO/IEC 29100] ISO/IEC 29100：2011年，信息技术 – 安全技术 – 隐私框架。

3 定义

3.1 他处定义的术语

本建议书使用以下他处定义的术语：

3.1.1 鉴权（authentication）[b-ISO/IEC 27000]：确保某个实体声称特征正确性的规定。

3.1.2 访问控制（access control）[b-ISO/IEC 10027]：限制使用访问已授权用户数据服务的能力。

3.1.3 控制（control）[b-ISO/IEC 27000]：修改**风险**（3.1.16）的措施。

注1 – 控制包括修改**风险**的任何**过程**（3.1.15）、**策略**（3.1.14）、设备、规程或其他行为。

注2 – 控制有可能不总是发挥预期或假定的修改效果。

3.1.4 设备（device）[b-ITU-T Y.4000]：在物联网中，具有强制性通信能力和选择性传感、激励、数据捕获、数据存储和数据处理能力的设备。

3.1.5 物联网（Internet of Things）（IoT）[b-ITU-T Y.4000]：信息社会的一种全球基础设施，基于现有的和正在演进的可互操作的信息和通信技术，实现（物理和虚拟）之物的相互连接，以提供先进的服务。

注1 – 通过使用标识、数据捕获、处理和通信能力，物联网充分利用物向各种各样的应用提供服务，同时确保满足安全和隐私要求。

注2 – 从广义而言，物联网可被视为技术和社会影响方面的一个愿景。

3.1.6 管理系统（management system）[b-ISO/IEC 27000]：一个**组织**（3.1.10）用于制定**策略**（3.1.14）和**目标**（3.1.7）以及实现这些目标的**过程**（3.1.15）中相互联系或相互作用的一组元素。

注1 – 管理系统可以管理一个科目或若干科目。

注2 – 系统元素包括组织的结构、职务和职责、规划和运作。

注3 – 管理系统的范围可以包括整个组织、组织的专门功能和已识别功能、组织的专门部门和已识别部门或整个组织集团中的一个或多个功能。

3.1.7 目标（objective）[b-ISO/IEC 27000]：需要取得的成果

注1 – 目标可以是战略目标、战术目标的或运作性目标。

注2 – 目标可以与不同的科目有关（例如财务目标、健康与安全目标、环境目标等），可以适用于不同的层次[例如，战略目标、组织目标、项目目标、产品目标和**过程**（3.1.15）目标）]。

注3 – 一个目标可以用其他方式表示，例如，表示为预期收入、用途、运行标准，或表示为信息安全目标或用其他具有类似含义的词汇表示（例如，目的、指标等）。

注4 – 在信息安全管理系统的范畴内，信息安全目标应由组织设定，应符合信息安全策略，以取得特定的结果。

3.1.8 选择加入（opt-in）[b-ISO/TS 17975]：借此可以要求数据主体采取单独的行动来表示明确同意、直接同意或优先同意某一特定处理类型的策略过程或类型。

3.1.9 选择退出（opt-out）[b-ISO/TS 17975]：借此可以要求数据主体为撤回对某一特定处理类型的许可而采取单独行动的策略过程或类型。

注 – 在选择退出的情况下，收集组织对个人信息的处理存在默示同意，除非个人明确否认或撤回许可。“选择退出”亦是数据收集组织提供的过程，目的是让数据主题拒绝或撤回执行某项特定处理的许可。

3.1.10 组织（organization）[b-ISO/IEC 27000]：有自己的职责、权限和关系以实现其**目标**（3.1.7）的个人或群体。

注 – 组织的概念包括但不限于个体商人、公司、法人、商号、企业、主管部门、合伙人、慈善团体或公共机构，或这些组织的组合体，不论是否是合营的，也不论是公有的还是私有的。

3.1.11 个人可识别信息（personally identifiable information）[ISO/IEC 29100]：（a）可用识别与此类信息相关的个人可识别信息主体；或者（b）直接或间接或者可能直接或间接与个人可识别信息主体联系起来的任何信息。

注 – 为确定个人可识别信息主体是否可以识别，应考虑持有该数据的隐私利益攸关方或任何其他方可合理使用的所有手段，以识别该自然人。

3.1.12 个人可识别信息首选项（personally identifiable information preferences） [ISO/IEC 29100]：由个人可识别信息（PII）主体就其个人可识别信息在某一特定目的下如何进行处理而做出的专门选择。

3.1.13 个人可识别信息主体（PII principal）[ISO/IEC 29100]：与个人可识别信息（PII）有关的自然人。

注 – 根据管辖权和专项数据保护和隐私立法的不同，可使用“数据主体”这一同义词替代“个人可识别信息主体”。

3.1.14 策略（policy）[b-ISO/IEC 27000]：由**最高管理层**（3.1.18）正式表达的一个**组织**（3.1.10）的意愿和方向。

3.1.15 过程（process）[b-ISO/IEC 27000]：一组相互联系或相互作用、将输入转化为输出的活动。

3.1.16 风险（risk）[b-ISO/IEC 27000]：不确定性对**目标**（3.1.7）产生的影响。

3.1.17 物（thing）[b-ITU-T Y.4000]：在物联网中，“物”指物理世界（物理事物）或信息世界（虚拟事物）中的一个对象，它可被标识并整合进通信网络中。

3.1.18 最高管理层（top management） [b-ISO/IEC 27000]：指导和控制**组织**（3.1.10）的个人或团体。

注1 – 最高管理层有权在组织中委托权力，并提供资源。

注2 – 如果**管理系统**（3.1.6）的范围仅覆盖组织的一部分，则最高管理层指的是指导和控制该部分组织的个人或团体。

注3 – 最高管理层有时被称为执行管理层，包括首席执行官、首席财务官、首席信息官以及类似的角色。

3.2 本建议书中定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用下列缩略语和首字母缩略词。

ACT 访问控制表

IoT 物联网

PII 个人可识别信息

T&C 条款和条件

5 惯例

无。

6 概述

物联网设备有很多种类型，其中一些设备能够收集个人可识别信息数据。由于个人可识别信息数据对于各种类型的服务都有用，所以，服务提供商特别注意从用户那里收集多种类型的个人可识别信息数据。此外，一个服务提供商可以与其他服务提供商共享这类收集到的个人可识别信息数据，以便集中为用户提供更有用的服务。在这种情况下，存在两种类型的服务提供商，一类服务提供商从用户那里收集个人可识别信息（PII）数据，另一类服务提供商利用其他服务提供商收集到的数据提供多种类型的服务。

从用户的角度看，其个人可识别信息数据应由这些服务提供商妥善处理。建议用户明确其数据在物联网环境下如何被处理的意图，包括个人可识别信息数据。在存在多个服务提供商的物联网环境下，因为数据使用情况比较复杂，所以应灵活兼顾用户数据使用的意图。例如，如果某个物联网服务提供商提供下列功能，则可以确认服务提供商收集和控制了通过正确渠道收集的数据（包括个人可识别信息数据）：

– 用户可以配置其自己的个人可识别信息首选项。这些首选项包括允许与其他服务提供商共享的数据列表。

– 应根据个人可识别信息首选项有控制地进行数据收集和共享。未授权的数据不能存储在数据存储器中，也不能在其他服务提供商之间共享。

– 用户可以检查服务提供商之间共享数据的历史日志。用户还可以检查数据共享的时间。

7 拥有单个或多个服务提供商的物联网服务模型

图1所示的是一个服务提供商提供一种服务的物联网服务模型。在这种情况下，服务提供商收集各种数据（包括个人可识别信息），并将信息存放在由服务提供商管理的数据存储器中。服务提供商为向服务提供商提供其个人数据（包括个人可识别信息）的用户提供各种类型的应用。

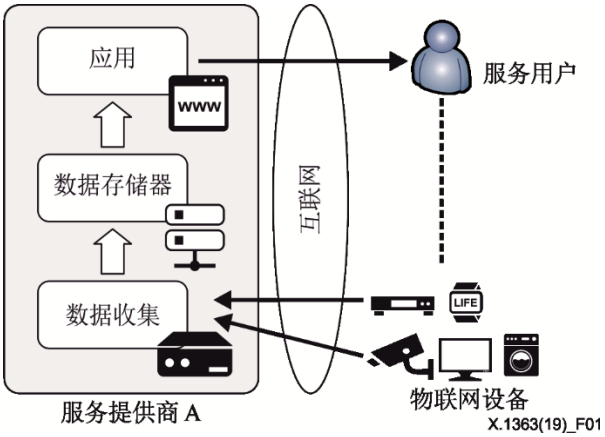

图1 – 单个服务提供商模型

在这个物联网服务模型中，单一服务提供商对收集到的数据进行处理，用户在约定的条款和条件（T&C）下使用具体的应用。

图2所示的是多个服务提供商共享通过物联网设备收集到的数据的模型。在这种情况下，存在两种服务提供商：“数据服务提供商”和“应用服务提供商”。在图2中，服务提供商A通过物联网设备收集数据（包括个人可识别信息），并与其他服务提供商（服务提供商B和服务提供商C）共享这些数据。服务提供商A的类型属于“数据服务提供商”，服务提供商B和C的类型属于“应用服务提供商”。一个服务提供商既可以是“数据服务提供商”，也可以是“应用服务提供商”。

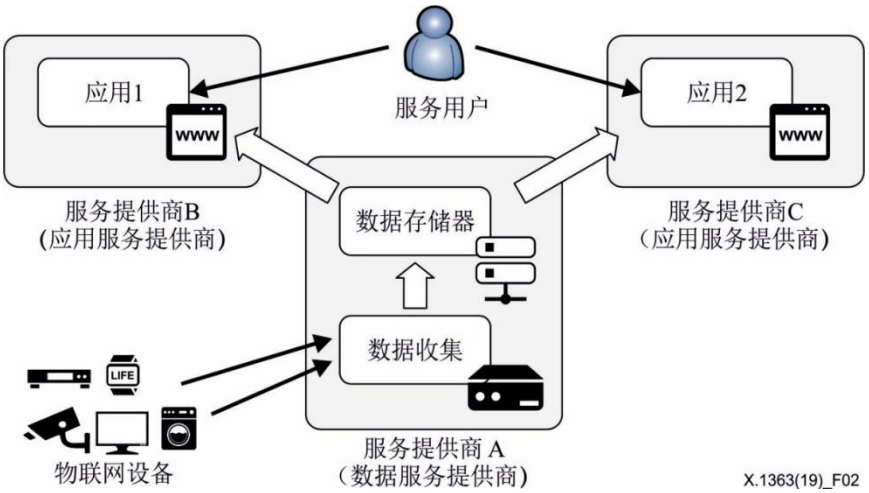

图2 – 多个服务提供商模型

通常，与其他服务提供商共享的数据列表包含在数据服务提供商的条款和条件中，用户在使用该服务提供商的服务前需要同意服务提供商的这些条款和条件。

单个服务提供商模型和多个服务提供商模型之间的主要区别在于物联网设备收集的数据是否与其他服务提供商共享。在多服务提供商模型中，物联网设备收集到的数据被传递给其他应用服务提供商。

8 物联网服务处理个人可识别信息数据的问题

处理个人可识别信息数据时，物联网服务提供商应考虑下列问题：

– 个人可识别信息数据收集的目的

从用户的角度看，为了避免出现不确定的用户观点数据收集，用户需要知道物联网服务的数据收集的目的和所收集的数据的特征。

– 个人可识别信息数据收集的强制性许可

当用户订购某一物联网服务时，数据服务提供商需要得到用户的许可来收集各种类型的个人可识别信息数据。通常，该信息在数据服务提供商的条款和条件中是列明的，用户在订购服务前必须同意这些条款和条件。

– 向第三方传递个人可识别信息数据

通过物联网设备收集到的数据可以与第三方（即，其他服务提供商）共享。在这种情况下，数据服务提供商在将个人可识别信息数据发送给其他服务提供商之前，需得到来自用户明确许可，允许将其个人可识别信息数据传递给第三方。在大多数情况下，用户不能控制个人可识别信息数据的传递。例如，用户不能选择其允许将个人可识别信息数据传输给哪个第三方，也不能配置哪一种个人可识别信息数据可以被共享。此外，用户不能知道什么样的个人可识别信息数据被传送给第三方。

– 个人可识别信息数据收集/传递许可的选择加入和选择退出

当某一服务使用用户个人可识别信息数据时，数据服务提供商需要从用户那里取得允许其从用户处收集个人可识别信息数据并将数据传递给第三方的许可。不仅收到许可的时间很重要，取得许可（选择加入或选择退出）的方法也很重要。

9 物联网服务处理个人可识别信息数据的原则

[ISO/IEC 29100]和[ITU-T X.1058]中规定了个人可识别信息保护原则和控制方法，个人可识别信息保护原则和控制方法是根据很多国家、州和国际组织，例如经济合作与发展组织（OECD）和亚太经合组织（APEC）的各种现有个人可识别信息保护原则而制定的。

第9.1和9.2条列出了物联网服务处理个人可识别信息数据的原则，以满足[ISO/IEC 29100]和[ITU-T X.1058]中的这些原则。

9.1 物联网服务处理个人可识别信息数据的一般原则

个人可识别信息可用于识别、联系或定位特定的个人。披露此类信息可能导致身份盗窃或其他欺诈性使用，给个人造成实质性伤害、困窘和不便[b-GAO-08-343]。因此，物联网服务对个人可识别信息数据的处理应符合以下一般原则：

1) 个人可识别信息数据的加密

所有保存在物联网设备或服务数据库中的个人可识别信息都应加密。此外，所有个人可识别信息在所有物联网服务组件（即物联网设备、数据存储和应用）内部和之间的传输过程中都应加密。

2) 访问控制/鉴权

如果个人可识别信息数据存储在物联网设备或服务数据库（数据存储器）中，应采用适当的访问控制。访问个人可识别信息的授权应仅限于在服务提供商提出同意请求的情况下实现其使用目的。这类使用目的应包括在服务提供商已获得用户同意的条款和条件中。当存储的数据集之间存在潜在的可链接性，可能导致对额外个人可识别信息的未授权标识或推断时，也应限制访问。

3) 日志记录

包括个人可识别信息数据在内的计算机可读数据摘要的创建应保存在正式日志中，包括创建者、日期、信息类型、提取目的和用户。在这些日志中包含的任何个人可识别信息（例如用户名）都应该被加密并服从访问控制。

4) 通信加密

如果个人可识别信息数据在多个服务提供商之间共享，则需要对其进行加密或屏蔽。

5) 数据泄露的通知

如果个人可识别信息数据在物联网服务中的任何点因数据泄露、透露、误用或处理不当而受到危害，服务提供商应在发现危害后立即通知受影响用户和相关服务提供商。

6) 数据保留的最小化程序

个人可识别信息数据的任何存储，无论是由服务提供商收集的还是作为数据处理的输出而产生的，均应仅限于服务提供商明确同意的特定目的。服务提供商应设置一个最大的受限个人可识别信息数据保留期限，设置依据是其规定的使用目的、存储的数据集之间存在任何链接进而导致识别或推断其他个人可识别信息的可能性以及和任何适用的国家法律法规。

9.2 个人可识别信息数据的处理原则

从物联网设备收集的个人可识别信息数据的数据服务提供商也应妥善处理个人可识别信息数据。特别是，如果数据被服务使用并在其他服务提供商之间共享，那么它的处理应该满足用户的意图。因此，物联网服务提供商对个人可识别信息数据的处理应遵循以下原则：

1) 收集个人可识别信息数据目的的解释

为了向用户收集提供某项物联网服务所需的最低必要个人可识别信息数据，服务提供商应在条款和条件中说明其收集目的以及收集的任何个人可识别信息的保留期限。

2) 明确同意收集和共享用户的个人可识别信息数据

服务提供商向用户提供PII数据采集服务时，应在数据采集和共享过程中征得用户明确的同意。特别是，服务提供商应在可能的情况下实施“选择加入”模式来征得同意。

3) 个人可识别信息数据使用的透明性

当个人可识别信息数据（包括服务提供商作为数据处理输出产生的任何个人可识别信息数据）在其他服务提供商之间共享时，服务提供商应提供透明的个人可识别信息管理机制，允许用户检查自己的个人可识别信息数据使用情况。物联网服务还应提供一种纠正机制，以便在发生数据错误归属时供用户使用。

4) 个人首选项的控制

个人可识别信息数据应根据用户配置的个人可识别信息首选项进行处理。

10 物联网环境下处理个人可识别信息数据

10.1 物联网环境下处理个人可识别信息数据的基本框架

图3所示的是物联网环境下处理个人可识别信息数据的基本框架。

首先，用户决定他们对个人可识别信息数据处理的首选项，并将其反映为他们在个人可识别信息首选项管理者中的个人可识别信息首选项。用户提供的数据（包括个人可识别信息）依据个人可识别信息首选项进行控制。

个人可识别信息首选项可以包括下列各项：

– 物联网设备收集的数据类型–物联网设备只能收集用户在其个人可识别信息首选项中专门许可的个人可识别信息数据。

– 物联网设备收集数据的时间（例如，每周工作日9：00~17：30）–用户不希望在任何时间发送其个人可识别信息数据，因此，这类时间需要在个人可识别信息首选项中进行配置。

– 允许共享个人可识别信息数据的服务提供商 – 用户可以选择能够访问其个人可识别信息数据的应用服务提供商。用户还可以选择该应用服务提供商能够访问的个人可识别信息数据种类，包括从物联网设备收集到的数据或主要服务提供商对数据处理后产生的输出数据。

当物联网设备、数据存储器、应用程序等物联网服务组件开始收集和使用数据时，应检查个人可识别信息首选项，并进行相应的处理。

其次，根据个人可识别信息首选项生成访问控制信息，并使用该信息更新访问控制表（ACT）。

第三，在收集或传输个人可识别信息数据时，每个组件都应参照这个访问控制表。访问控制表中的访问控制信息用于控制在物联网服务组件之间可以传输何种类型的个人可识别信息数据。

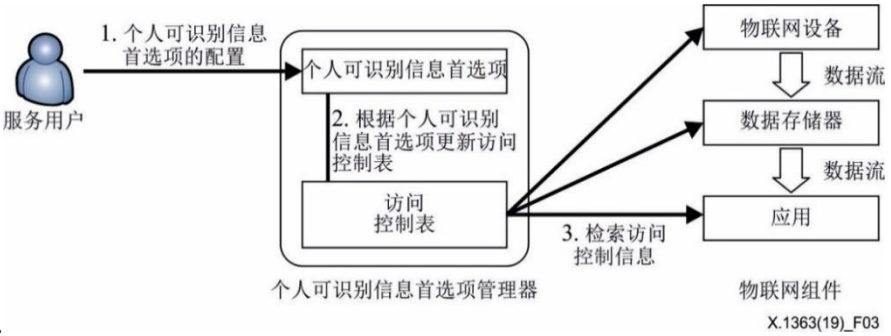

图3 – 个人可识别信息数据处理的基本框架

10.2 配置个人可识别信息首选项用户接口的原则

为了实施此基本框架，服务提供商应提供一个配置个人可识别信息首选项的用户接口。该用户接口符合下列原则：

1) 对于所有用户都易于访问

所有用户都应很容易地访问用户接口。例如，所提供的服务的第一个界面应链接到此用户接口。

2) 对用户接口有适当的访问控制

每个服务用户有其自己的个人可识别信息首选项。因此，每个用户应有唯一的用户账号，并应以安全的方式进行认证，例如，在允许用户访问其账号前，应设置两个因素的认证。

3) 综合性

用户接口应管理所有的个人可识别信息首选项，包括一个位置上一个用户的个人可识别信息收集的首选项和共享的首选项。

4) 易于使用

用户接口应方便用户直接配置其个人可识别信息首选项。

11 物联网环境下处理个人可识别信息数据的技术框架

本条规定了如何在单个和多个服务提供商环境中使用第10条规定的个人可识别信息数据处理的基本框架。

11.1 物联网环境中由单个服务提供商处理个人可识别信息数据

11.1.1 单个服务提供商提供的物联网服务参考模型

图4所示的是由单个服务提供商提供的物联网的服务的参考模型。在这种情况下，一个服务提供商为物联网服务提供所有功能。服务提供商从物联网设备收集数据（包括个人可识别信息），并将之存放在其数据存储器中。利用收集到的数据可以将应用服务提供给用户。

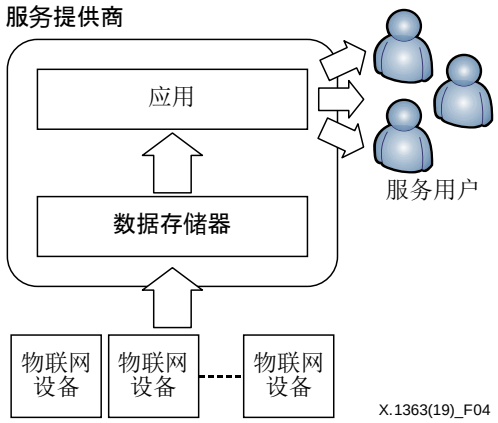

图4 – 单个服务提供商提供物联网服务的参考模型

11.1.2 单个服务提供商处理个人可识别信息数据的技术框架

图5所示的是拥有管理用户个人可识别信息首选项的个人可识别信息首选项管理器的服务提供商技术框架。用户利用该个人可识别信息首选项管理器配置其个人可识别信息首选项，如物联网设备、数据存储器和应用等物联网服务组件根据配置对个人可识别信息数据进行配置。例如，如果一个用户想要限制通过物联网设备收集特殊的个人可识别信息数据，则物联网设备不得将个人可识别信息数据发送给数据存储器。

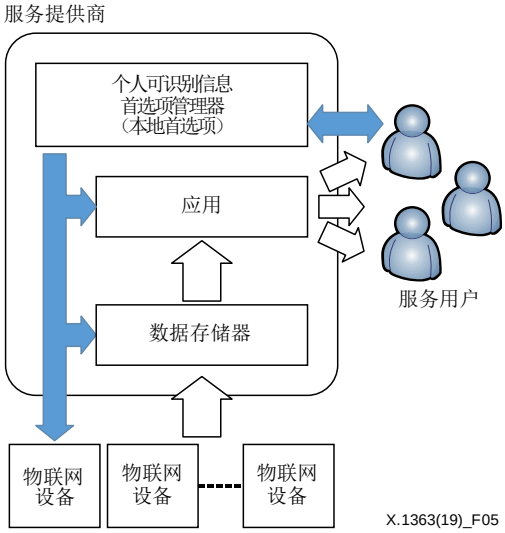

图5 – 单个服务提供商处理个人可识别信息数据的技术框架

11.1.3 单个服务提供商用通用个人可识别信息首选项管理门户处理个人可识别信息数据的技术框架

当物联网服务由单一服务提供商提供时，物联网设备收集的数据不会与物联网服务不被用户使用的其他服务提供商共享。然而，服务提供商之间需要共享个人可识别信息首选项中的一些常见基本项目，因为用户为每个物联网服务配置其个人可识别信息首选项可能会花费太多时间。如果用户可以为任何类型的物联网服务指定通用个人可识别信息首选项，那么为每个单独的服务配置个人可识别信息首选项将更容易、更有效。为实现之，有两种类型的个人可识别信息首选项管理器。

图6是一个显示有两个个人可识别信息首选项管理器组件的技术框架,一个仍是位于一个服务提供商处的个人可识别信息首选项管理器，另一个是个人可识别信息首选项管理门户，用于管理任何物联网服务和其他服务提供商访问的一般首选项。

在这种情况下，用户对任何服务的通用首选项设置存储在个人可识别信息首选项管理门户中，而用户对每个服务的特定首选项设置存储在由每个服务提供商管理的个人可识别信息首选项管理器中。当用户开始订阅新的服务时，数据服务提供商的本地个人可识别信息首选项管理器将从个人可识别信息首选项管理门户检索其通用设置，该门户可以由第三方管理并由用户预先配置。尽管用户仍然需要使用本地个人可识别信息首选项管理器为该特定服务配置其个人可识别信息首选项，但其不需要每次都配置存储在个人可识别信息首选项管理门户中的通用首选项。物联网服务组件，如物联网设备、数据存储和应用程序，在个人可识别信息首选项管理器中根据本地设置来控制个人可识别信息数据。

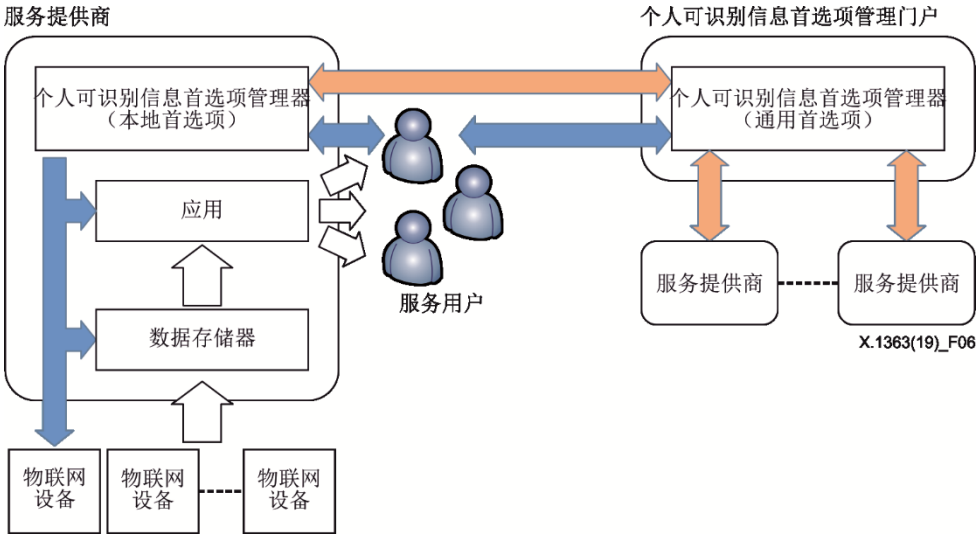

图6 – 拥有通用个人可识别信息首选项管理门户的单个服务提供商处理个人可识别信息数据的技术框架

11.2 多个服务提供商处理物联网服务中的个人可识别信息数据

11.2.1 多个服务供应商提供物联网服务的参考模型

图7是一个描述多个服务提供商提供物联网服务的参考模型。在这种情况下，物联网服务由多个服务提供商（应用服务提供商和数据服务提供商）组成，每个应用服务提供商通过使用其他数据服务提供商收集的数据向用户提供自己的服务。因此，从物联网设备（数据服务提供商）收集数据（包括个人可识别信息）的服务提供商可以不同于只向用户提供服务的服务提供商（应用服务提供商）。在图7中，有两种类型的服务提供商，一种是从物联网设备收集数据（包括个人可识别信息）的“数据服务提供商”，另一种是使用收集的数据向用户提供应用服务的“应用服务提供商”。

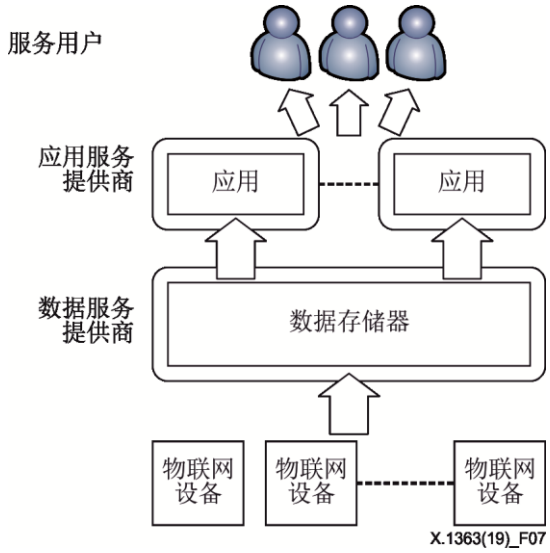

图7 – 多个服务提供商提供物联网服务的参考模型

11.2.2 多个服务提供商处理个人可识别信息数据的技术框架

图8是一个技术框架，其中显示数据服务提供商有一个个人可识别信息首选项管理器，处理个人可识别信息数据所使用的所有用户首选项设置都在这个本地管理组件中进行管理。用户使用个人可识别信息首选项管理器配置他们的本地首选项设置。物联网服务组件（包括其他应用服务提供商提供的应用程序）根据数据服务提供商的个人可识别信息首选项管理器中的本地首选项设置处理个人可识别信息数据。

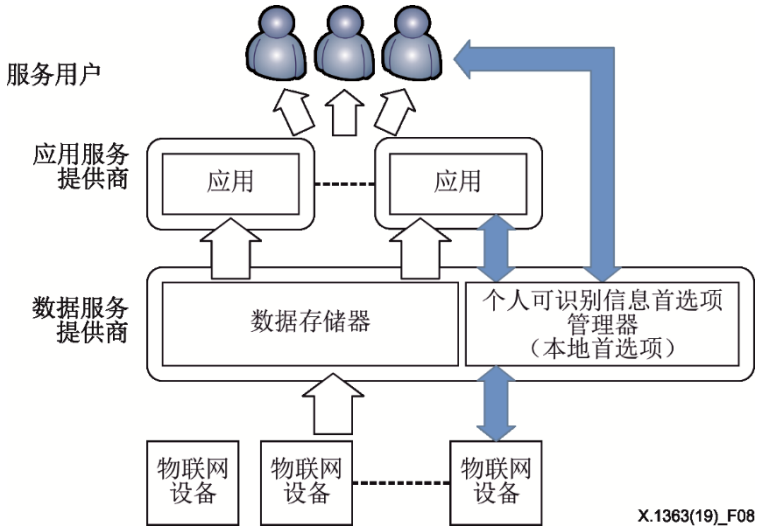

图8　　多个服务提供商提供物联网服务的个人可识别信息数据处理技术框架

11.2.3 多个服务供应商提供物联网服务中使用一个通用个人可识别信息首选项管理门户处理个人可识别信息数据的技术框架

图9是一个技术框架，显示了多个服务提供商同时使用存储在通用个人可识别信息首选项管理门户和数据服务提供商的本地个人可识别信息首选项管理器中的个人可识别信息首选项。

在这种情况下，任何服务的通用首选项存储在通用个人可识别信息首选项管理门户中，而每个服务的特定首选项存储在由每个数据服务提供商管理的本地个人可识别信息首选项管理器中。当用户开始订阅新的服务时，服务提供商的本地个人可识别信息首选项管理器将从个人可识别信息首选项管理门户中检索通用首选项。尽管该用户仍然需要在本地个人可识别信息首选项管理器中配置其个人可识别信息首选项，但是不需要重复配置存储在个人可识别信息首选项管理门户中的通用个人可识别信息首选项。物联网服务组件基于个人可识别信息首选项管理器中的本地首选项设置来控制个人可识别信息数据。

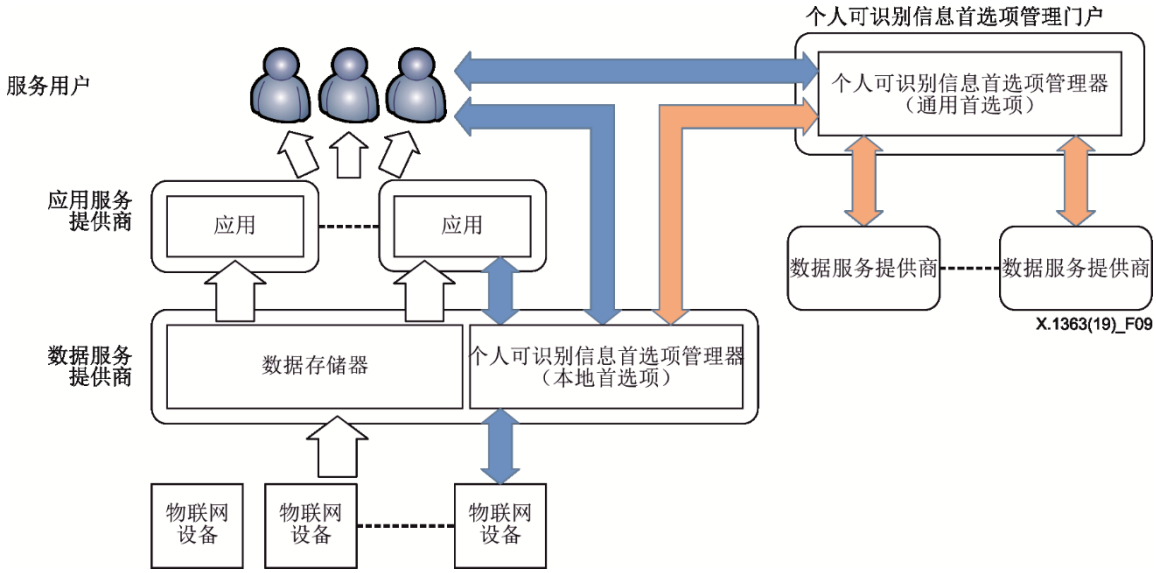

图9 – 多个服务提供商提供物联网服务中用通用个人可识别信息首选项管理门户处理个人可识别信息数据的技术框架

参考书目

[b-ITU-T Y.4000] ITU-T Y.4000/Y.2060建议书（2012年），物联网概述。

[b-ISO/IEC 10027] ISO/IEC 10027:1990*Information technology – Information Resource Dictionary System (IRDS) framework*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[b-ISO/TS 17975] ISO/TS 17975:2015, Health informatics -- Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information

[b-GAO-08-343] GAO-08-343 (2008). *Information security: Protecting personally identifiable information*. Washington, DC: United States Government Accountability Office. 34 pp.

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2020年，日内瓦