



研究与开发

网络环境中的隐私保护标准化研究^{*}

高 枫¹, 张 峰², 周 伟¹

(1. 中讯邮电咨询设计院有限公司 北京 100048;

2. 北京邮电大学智能通信软件与多媒体北京市重点实验室 北京 100876)

摘 要: 随着网络应用的不断丰富,越来越多的网络应用中涉及各种隐私信息,隐私保护标准化成为业界的研究热点。通过对国内外标准化组织在网络环境中隐私保护工作的归纳梳理,分析了当前隐私保护标准化工作的主要特点、难点和重点,并在此基础上探讨了隐私保护标准化发展的趋势。

关键词: 网络;隐私保护;标准化

doi: 10.3969/j.issn.1000-0801.2013.04.022

Study on Standardization of Privacy Protection in Network Environment

Gao Feng¹, Zhang Feng², Zhou Wei¹

(1. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China;

2. Beijing Key Laboratory of Intelligent Telecommunications Software and Multimedia,
Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: With the development of network technology and its broad applications, more and more applications involve privacy. Therefore, standardization of privacy protection becomes a hot topic. Privacy protection work by international standard organizations was introduced, and then the main features, and difficulty and key points for that were analyzed. According to the analysis, the trend of standardized work in privacy protection was also discussed.

Key words: network, privacy protection, standardization

1 引言

中国互联网络信息中心(CNNIC)发布的第31次《中国互联网络发展状况统计报告》显示,截至2012年12月底,我国网民规模达到5.64亿,互联网普及率为42.1%。网络的普及为信息共享和交互提供了极大的便利。

随着下一代互联网、移动P2P网络、物联网、泛在网络、社交网络、云计算等各种新型网络及应用的出现,越来越多

的网络应用中涉及各种隐私信息。当前网络环境中共享、存储和管理的隐私信息规模急速增长,收集、利用隐私信息的技术迅速发展^[1],这些都使得网络环境中的隐私保护更加复杂和困难,隐私保护问题日益受到学术界和工业界的广泛关注。

为应对隐私保护的需求,目前国际上已有众多标准组织及产业联盟启动了隐私保护的标准化工作,本文将从隐私保护标准化的现状入手,分析隐私保护标准化的特点、方向与趋势。

^{*} 国家自然科学基金资助项目(No.61074128),中国联通集团设计院研究项目(No.2013YF0009)

2 隐私保护国内外标准化现状

目前,国内隐私保护相关的外标准化工作已经启动,ISO/IEC(国际标准化组织/国际电工委员会)、OMA(开放移动联盟)、3GPP(第三代合作伙伴项目)、GSMA(全球移动通信系统协会)、W3C(万维网联盟)、CCSA(中国通信标准化协会)等国内外标准化组织,从不同角度就网络环境中的隐私保护制定了相关标准^[3],具体见表1。

2.1 ISO/IEC

ISO/IEC JTC1 SC27(信息安全分技术委员会)^[4]WG5组(身份管理和隐私保护技术工作组)主要研究和制定身份管理、生物特征以及个人数据保护相关的标准。WG5在隐私保护方面的主要工作如下。

- ISO/IEC 29100 Privacy Framework(隐私框架),其基本元素包括主体、个人身份信息、风险、隐私偏好、隐私需求和隐私原则。框架定义了隐私保护的要求、通用的隐私术语、规范处理个人身份信息的隐私原则,对隐私保护功能进行了分类,形成一个可行的隐私标准化的基础框架,包括技术性的参考架构、隐私技术的使用、整体隐私管理、外包数据处理隐私保证、隐私性评估以及工程规范等^[5]。ISO/IEC 29100 隐私保护框架结构如图1所示。
- ISO/IEC 29101 Privacy Reference Architecture(隐私参考体系架构),该架构提供了隐私保护技术实施的指导,用于信息通信系统建设。ISO/IEC 29101 隐私保护参考架构。
- ISO/IEC 29190 Privacy Capability Assess Model(隐私能力评估模型),提供了高层次的指导,评估隐私管

理的成熟度。

- ISO/IEC 29191 Requirements for Partially Anonymous, Partially Unlinkable Authentication(部分匿名和部分不可连接认证的需求),提供身份代管的不可连接匿名认证的模型及需求。其目的是提供群组签名和相关机制的指导,减少数据量并提升用户体验,同时允许用户通过其托管代理控制用户匿名性。

2.2 OMA

OMA针对移动网络应用提出了基本的隐私保护要求,在2007年发布了OMA Privacy Requirements for Mobile Services V1.0(OMA移动服务的隐私需求)^[6]。

在OMA体系中,每个服务可能有自己的隐私需求,并用自己的方式解决。例如,位置服务可以根据存储的用户偏好,在用户进入某一区域时执行操作,向其他人发送信息。因此,OMA规范旨在通过收集相同的需求为OMA服务创建通用的解决方法。该规范明确了隐私策略的执行对OMA体系的影响,提出隐私策略应从内容提供商的角度表明使用的意图,包括目的、收件人、保留期,并指出如何与数据处理器通信以及对争议的处理等。

2.3 3GPP

3GPP TR 22.949 Study on a Generalized Privacy Capability(通用隐私能力的研究)^[7]研究了通用隐私能力。其范围包括:明确3GPP系统相关的隐私信息;明确现有3GPP服务应如何处理隐私相关信息;明确隐私相关角色,明确个人数据在这些角色中的处理流程;明确隐私角色的各种行为规范等。

2.4 GSMA

随着移动应用、服务和数据的国家化,基于地理位置

表1 国内外隐私保护相关标准化成果统计

标准组织	题目	发布时间
ISO/IEC	ISO/IEC 29100 Privacy Framework(隐私框架); ISO/IEC 29101 Privacy Reference Architecture(隐私参考架构); ISO/IEC 29190 Privacy Capability Assess Model(隐私能力评估模型); ISO/IEC 29191 Requirements for Partially Anonymous, Partially Unlinkable Authentication(部分匿名和部分不可连接认证的需求)	2011年
OMA	OMA Privacy Requirements for Mobile Services V1.0(OMA移动服务的隐私需求)	2007年
3GPP	3GPP TR 22.949 Study on a Generalized Privacy Capability (R11)(通用隐私能力的研究)	2012年
GSMA	Mobile Privacy Principles(移动隐私原则); Privacy Design Guidelines for Mobile Application Development(移动应用开发的隐私设计原则)	2011年
W3C	Device API Privacy Requirement(设备API的隐私需求); Web Application Privacy Best Practice(Web应用隐私最佳实践); Privacy Ruleset(隐私规则集合)	2009年 2011年 2009年
CCSA	身份管理(IdM)术语;移动终端安全能力技术要求;移动终端安全能力测试方法	2012年

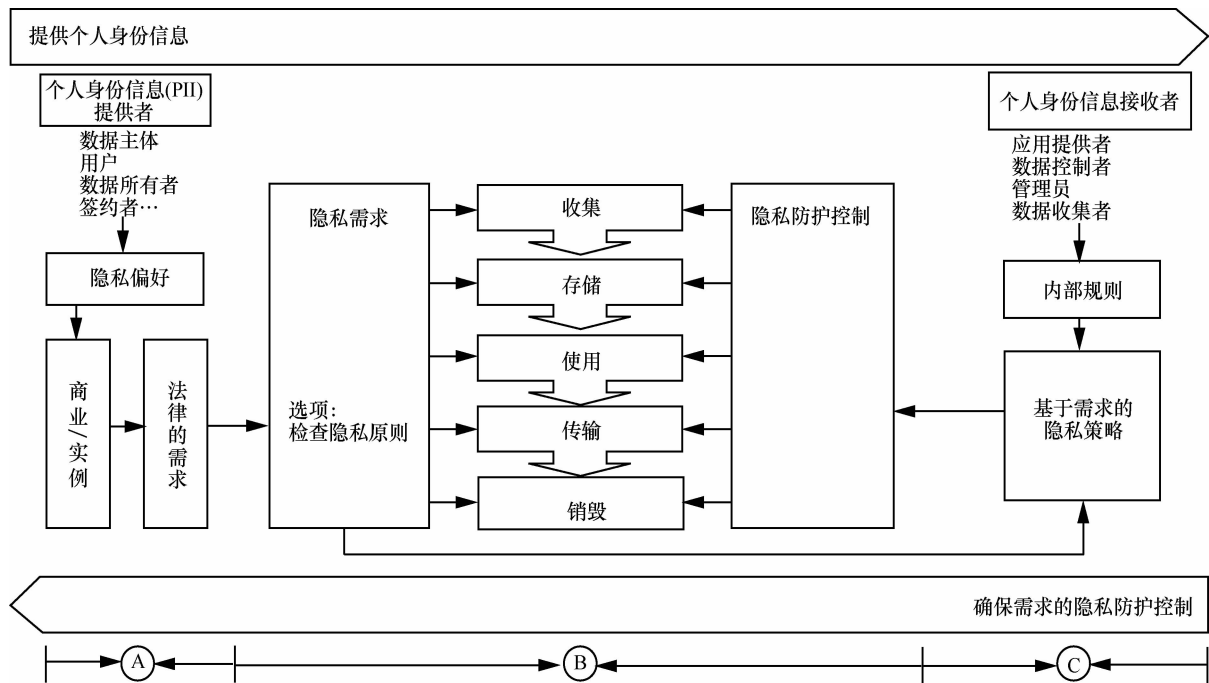


图 1 ISO/IEC 29100 隐私保护框架

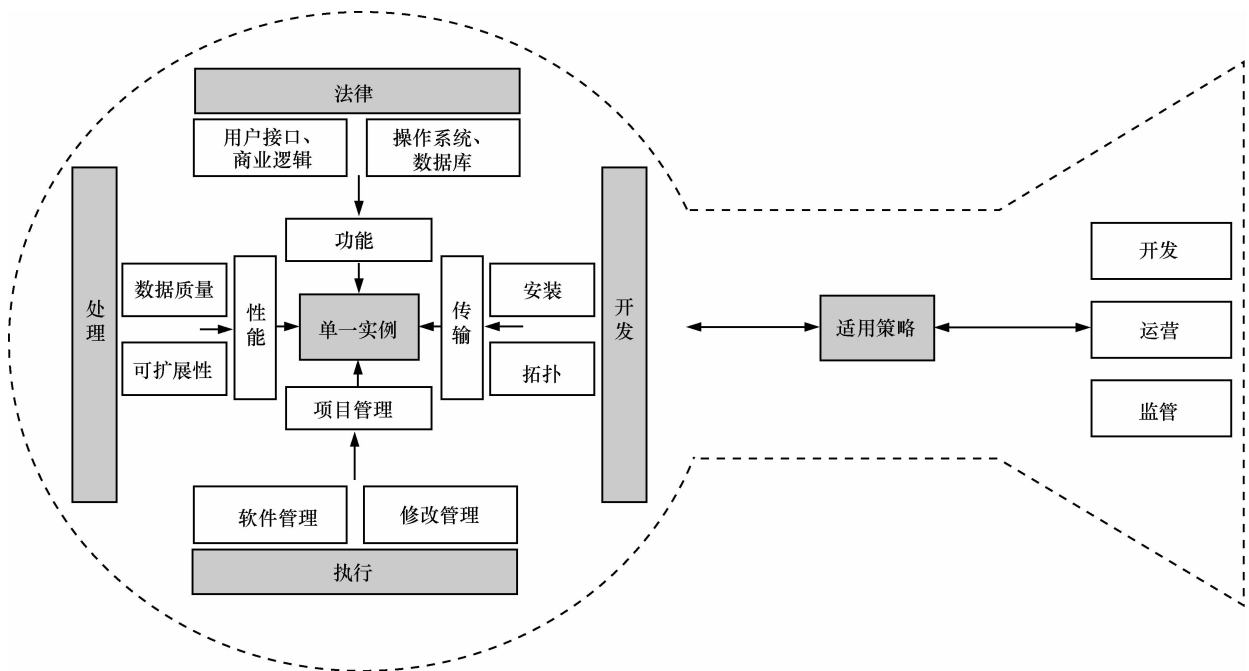


图 2 ISO/IEC 29101 隐私保护参考架构

的数据隐私保护规则无法满足移动互联网的需求, 据此, GSMA 启动了移动隐私计划^[9], 旨在确保消费者隐私在各种移动应用、平台及服务中得到更加一致的处理并继续支持创新, 达成广泛共识。

2011 年 1 月 27 日 GSMA 发布了 Mobile Privacy Principles (移动隐私原则)^[9], 原则明确了在用户使用需要访问、使用

或采集个人信息的移动应用及服务时, 移动用户隐私应当受到尊重和保护。原则将用于制定更为详尽的指导方针和行为准则, 以解决用户关心的应用程序使用个人资料等具体问题, 为用户管理其手机上的信息及隐私制定明确简单的方法提供指导。

GSMA 同时发布了 Privacy Design Guidelines for Mobile

Application Development(移动应用开发的隐私设计原则)^[10],该规范将“移动隐私原则”应用于移动终端服务的设计中,旨在将隐私保护用于移动互联网应用的全链条中,从而建立一个可信的移动生态系统。

2.5 W3C

W3C 主要关注于 Web 领域的隐私问题,积极推进隐私保护的标准化工作。

W3C 隐私兴趣组^[11]研究影响 Web 用户隐私的各种行为,兴趣组将输出相应的导则、模型、过程和最佳实践,以指导涉及隐私保护的 W3C 标准的制定。

W3C 跟踪保护工作组^[12]定义了机器可读的隐私偏好的跟踪(track)使能策略,通过扩展 HTTP 分组头,采用 ECMAScript API 或 DOM 方法提供用户偏好配置机制。

W3C DAP(device API and policy)工作组^[13]旨在制定移动终端侧 API,互联网应用与终端提供的服务通过 API 进行交互。同时,该工作组还研究制定了安全框架,该框架管理用于对 API 的安全访问/调用。工作组在隐私保护方面主要有 3 个标准草案:Device API Privacy Requirement(设备 API 的隐私需求)^[14]、Web Application Privacy Best Practice(Web 应用隐私最佳实践)^[15]和 Privacy Ruleset(隐私规则集合)^[16]。

2.6 CCSA

CCSA 在隐私保护标准化研究工作中,主要体现在身份管理和移动终端安全等方面。

CCSA TC8 WG4 制定了身份管理的系列标准,包括体系架构、术语、数据模型、接口消息技术要求、互通技术要求等。

CCSA TC11 WG3 制定了《移动终端安全能力技术要求》和《移动终端安全能力测试方法》,对移动终端用户数据安全保护能力做出了相关要求,包括移动终端的密码保护,用户数据的加密存储、授权访问、远程保护及转移备份等。

3 隐私保护标准化的特点

3.1 标准化内容日趋丰富

从目前标准化组织输出的成果来看,隐私保护标准化内容日趋丰富,工作主要涵盖以下几个方面。

(1) 隐私信息分类

目前标准组织将隐私信息普遍定义为个人数据,包括绑定到数据主体的信息(如地址、电话号码)、与其他数据相结合可以推测出数据主体身份的信息(如 IP 地址)、有特定要求而存储的信息(如 cookies 和位置数据)等。

(2) 隐私角色

尽管各个标准组织对隐私信息保护研究的侧重点不同,但对于隐私保护中的角色划分大体一致,可以归纳为数据主体、个人信息以及接收者/使用者三大类。此外,根据标准组织研究的不同侧重点,又可细分为本地运营商、服务提供商、移动应用等。

(3) 隐私处理规则

隐私处理规则是隐私保护的核心,标准组织相关的隐私保护标准中大都对处理规则做出了明确要求。隐私规则可以归纳为以下几类:

- 隐私偏好,大多标准都允许用户对其隐私偏好设定;
- 访问规则,即定义“什么人”可以用“怎样的处理权限”访问“什么样的个人数据”;
- 处理权限,即定义对访问个人数据的权限控制。

(4) 隐私原则

隐私原则是对业务和系统开发中隐私信息处理的指导,抽取各标准组织隐私原则的共性,可以归纳为以下几点:

- 公开、透明化与通知,即为用户提供明确、及时的数据隐私信息,用户应知道何种个人信息被采集及其原因以及这些信息的访问、存储、分享及未来的使用方式,使用户能对数据使用做出选择;
- 目的与使用,即用户个人信息的访问、存储、分享及未来使用应限于合法的商业目的,为用户提供便利或满足法律的义务;
- 最小化个人信息,即应用所收集的个人信息应该适量,而不能过量,且信息的使用应在用户要求和法律规定的范围内。

3.2 隐私保护范围成为标准化难点

随着网络技术的不断发展和广泛应用,隐私已由纯粹的社会学问题演化为兼具技术与社会双重属性的复杂问题。网络环境中的隐私是集社会、法律、技术等因素为一体的综合性概念。隐私概念没有标准定义,但强调个人对其隐私信息的控制能力。

网络环境中的隐私保护内容不仅涵盖传统的私人信息,同时还包括实体参与网络活动所产生的数字行为和通信内容等。数字行为如浏览了哪些网站、停留了多长时间、在哪些网站订购了哪些商品等;通信内容如电子邮件内容、即时通信内容等。由此产生的动态隐私和衍生隐私,也是网络环境中隐私保护的内容。Corby 在《The Case for Privacy》^[17]一文中将隐私进行了分类,如表 2 所示^[18]。



表 2 隐私分类

隐私数据类型			子类型
静态隐私	身份数据	物理身份数据	· 生物特征信息,如指纹、瞳孔、身高、肤色、体貌特征等; · 财务信息,如银行账号密码、信用卡账号等; · 法律信息,如身份证号、驾驶执照编号等; · 社会信息,如政治党派、民族等; · 关系信息,如子女、父母、配偶等亲属关系等; · 真实住址信息,如家庭住址、公司地址等
		网络身份数据	通常为数字信息,如用户名、电子邮件、IP 地址、密码等
	资产数据	有形资产	· 不动产,如房产、车子等; · 个人财务信息,如信用卡账单、购物清单、债务清单等
		无形资产	通常为非物质财产,如保险单、工作合同等
动态隐私	历史数据		· 低识别度信息,如使用过的服务、兴趣爱好等; · 高识别度信息,如在某一时间所处的位置信息等
	实时数据		实时信息,如当前时间所处的位置等
衍生隐私	分析数据		通过对历史数据的分析统计得到的信息,通常为趋势、变化、爱好、社会关系等信息的预测
	组合数据		通过组合数据信息得到的用户个人信息,如通过 DNA 信息可以找到用户的基因信息,从而发现用户的疾病状况等

隐私具有个性化的特点,不同实体对隐私的内涵、外延、敏感度等理解不同,同一实体在不同网络环境中的隐私保护需求也不尽相同,呈现出多样性的特点。随着网络应用的日益丰富,各个标准组织在制定隐私保护相关标准时业务相关的侧重点不尽相同,加之隐私保护的多样性特点,使得隐私保护标准化工作中的隐私保护范围难以达成较为一致的共识,隐私保护范围成为标准化的难点。

3.3 隐私保护原则及处理规范是标准化重点

隐私保护处理规范明确对访问个人数据的权限控制,定义“什么人”可以用“怎样的处理权限”访问“什么样的个人数据”是隐私保护的核心。隐私保护原则用于制定更为详尽的指导方针和行为准则,是对业务和系统开发中隐私信息处理的指导。目前,标准组织输出的隐私保护相关标准中大都对隐私保护原则和处理规则做出了明确要求,然而,随着业务多样性的不断演化以及收集、利用隐私信息的技术迅速发展,有效满足业务场景和需求的隐私保护原则及处理规范将成为今后标准化工作的重点。

4 隐私保护标准化发展趋势

因各标准组织的工作侧重点不同,隐私保护的关注点应该也有所不同。由于隐私信息的多样性特点,使得相同类别的隐私信息在不同业务场景下的保护需要不尽相同,因此,很难使用统一的标准涵盖网络环境的各种业务的隐私保护需求。

随着下一代互联网、移动 P2P 网络、物联网、泛在网络、社交网络、云计算等各种新型网络及应用的出现,越

来越多的网络应用中涉及各种隐私信息。在业务细分前提下的隐私保护标准化,将成为未来标准化工作的主要方向。

因此,在未来的隐私保护相关的标准化工作中,个性化的隐私保护标准、业务细分前提下的隐私保护标准都将成为标准化发展的趋势。

5 结束语

随着网络应用的不断丰富和发展,越来越多的应用中涉及隐私信息。国内外标准组织开展了隐私保护标准化工作,ISO/IEC、OMA、3GPP、GSMA、W3C、CCSA 等国内外标准化组织从不同角度就网络环境中的隐私保护制定了相关标准,用于业务和系统开发中隐私信息处理的指导。随着网络应用的不断丰富,不断研究适用于新业务、新场景的隐私保护标准将成为标准化组织的工作内容。在未来的隐私保护相关的标准化工作中,个性化的隐私保护标准、业务细分前提下的隐私保护标准化都将成为标准化发展的趋势。

参考文献

- 1 Vanja S, Borka J B, Tomaz K. Privacy-enhancing technologies approaches and development. Computer Standards & Interfaces, 2003, 25(2):147~158
- 2 Edman M, Yener B. On anonymity in an electronic society: a survey of anonymous communication systems. ACM Computing Surveys, 2009, 42(1): 1~35
- 3 CCSA 研究报告.移动互联网用户隐私保护技术研究,2012

- 4 ISO/IEC JTC 1/SC 27. <http://www.jtc1sc27.din.de/>
- 5 ISO/IEC JTC 1/SC 27. Working Group 5 Identity Management and Privacy Technologies within ISO/IEC JTC 1/SC 27-IT Security Techniques, 2007
- 6 OMA Privacy Requirements for Mobile Services. http://www.openmobilealliance.org/technical/release_program/privacy_v1_0.aspx, 2007
- 7 3GPP TR 22.949. Study on a Generalized Privacy Capability, 2012
- 8 GSMA Mobile Privacy Initiative. <http://www.gsma.com/mobile-and-privacy/>
- 9 GSMA Mobile Privacy Principles. http://www.gsmworld.com/documents/GSMA_Privacy_Principles_UPDATED.pdf, 2011
- 10 GSMA Privacy Design Guidelines For Mobile Application Development. http://www.gsmworld.com/documents/privacy_design_guidelines.pdf, 2011
- 11 W3C Privacy Interest Group Charter. <http://www.w3.org/2011/07/privacy-ig-charter.html>
- 12 W3C Tracking Protection Working Group. <http://www.w3.org/2011/tracking-protection/>
- 13 W3C Device APIs and Policy Working Group. <http://www.w3.org/2009/dap/>
- 14 W3C Device API Privacy Requirement. <http://www.w3.org/TR/2010/NOTE-dap-privacy-reqs-20100629/>, 2009
- 15 W3C Web Application Privacy Best Practice. <http://www.w3.org/TR/2011/WD-app-privacy-bp-20110804/>, 2011
- 16 W3C Privacy Ruleset. <http://dev.w3.org/2009/dap/privacy-rulesets/>, 2009
- 17 Corby M J. The case for privacy. Information Security Journal: A

Global Perspective, 2002, 11(2):9~14

- 18 刘恒. 普适计算环境下基于位置服务的隐私保护若干技术研究. 电子科技大学博士学位论文, 2010

[作者简介]



高枫,女,博士,中讯邮电咨询设计院有限公司工程师,主要研究方向为 3GPP 标准和 EPC 技术。



张峰,男,北京邮电大学博士研究生,主要研究方向为移动网络和智能信息处理。



周伟,男,博士,中讯邮电咨询设计院有限公司高级工程师,主要研究方向为 3GPP 标准和移动互联网。

(收稿日期:2013-02-05)

(上接第 111 页)

张曦,男,空军工程大学航空航天工程学院讲师,主要研究方向为信息网络对抗技术等。

闫涛,男,博士,空军第一航空学院讲师,主要研究方向为信息通信网络等。

王红卫,男,博士,空军工程大学航空航天工程学院副教授、主任,主要研究方向为信息对抗技术等。

钟永信,男,博士,94850 部队工程师,主要研究方向为水声传感器网络等。