隐 私 数 据 的 前 世 今 生

——浅析个人数据保护

中国金融认证中心信息安全实验室

高强裔

2016年10月31日

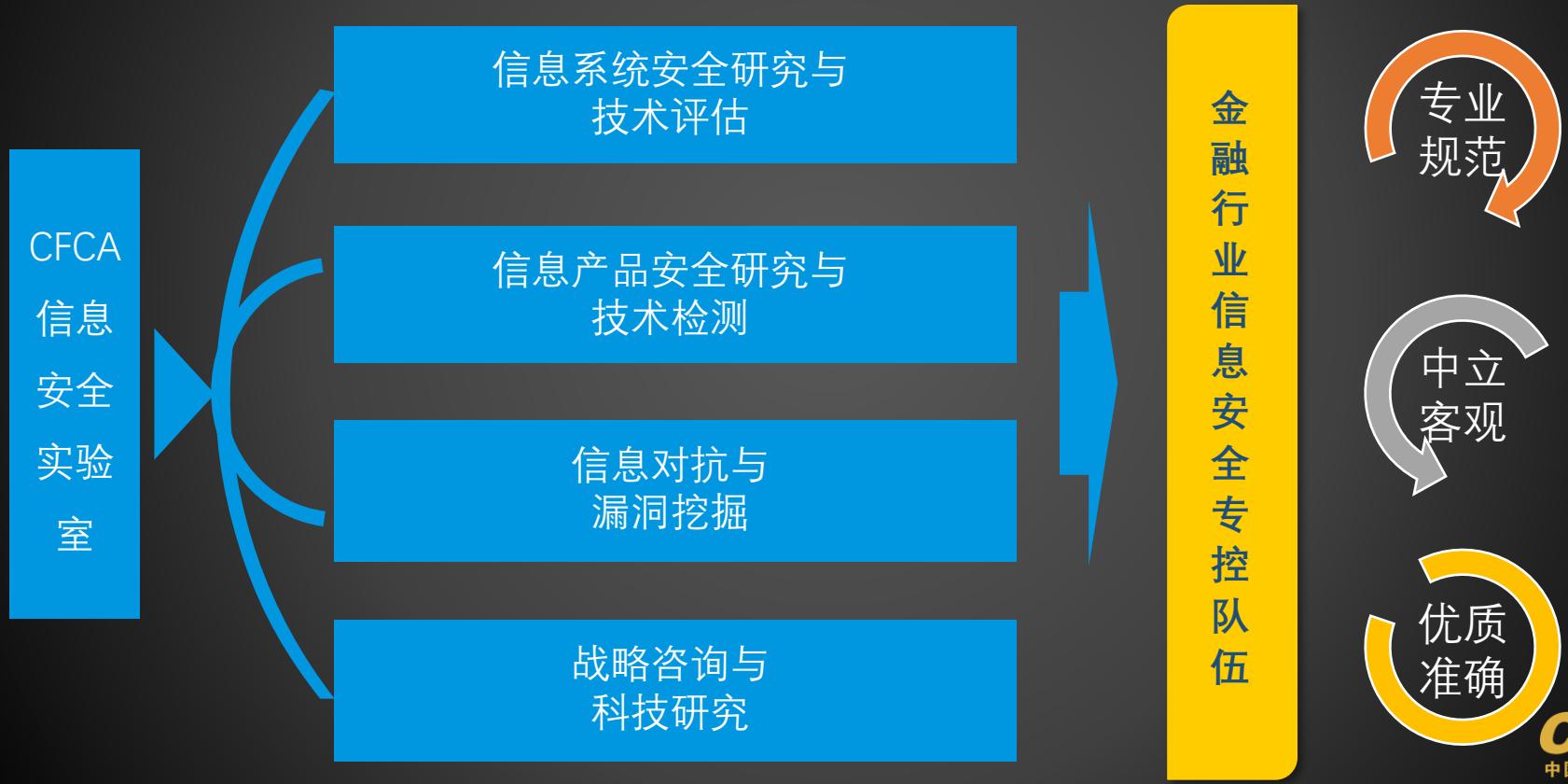
CFCA
中国金融认证中心

写在最前面

关于CFCA信息安全实验室

中国金融认证中心信息安全实验室(CFCA信息安全实验室)

- 依托CFCA信息安全服务部的人员与技术能力，公司组建中国金融认证中心信息安全实验室（简称“CFCA信息安全实验室”）
- 作为**公正、独立**的**第三方机构**，立足于银行业机融机构，面向广大金融行业，提供系统级与产品级的安全评估与检测工作。



主管部门与监管部门技术支撑

- 作为行业主管部门与监管部门的技术支撑单位、金融行业信息安全专控队伍，CFCA多次参加主管部门行业标准制定、产业技术调研工作，为包括人民银行、银监会、国家密码管理局等主管部门与业务指导单位提供技术支撑与一线技术应用信息反馈。

参与制定国家、行业标准名录（部分）

序号	参与制定标准/规范名称	该标准归口部门	CFCA参与角色
1	“中国金融移动支付”系列标准初始制定，以及后续修订项目	人民银行	主要编写单位
2	JR/T 0068《网上银行系统信息安全通用规范》标准修编	人民银行	主要参与单位
3	JR/T 0025系列 “中国金融集成电路（IC）卡规范”系列标准修订与增补项目	人民银行	主要参与单位
4	《非金融机构支付服务业务系统检测规范》	人民银行	主要参与单位
5	“电子支付”系列标准	人民银行	主要参与单位
7	JR/T 0142《银行卡清算业务设施技术要求》制定项目	人民银行	主要参与单位
8	“中国金融移动支付”系列《支付标记化技术规范》制定项目	人民银行	主要参与单位
9	“银联卡账户信息安全合规评估”、《第三方机构接入中国银联技术安全规范》	中国银联	主要参与单位
10	“银行业业务系统信息安全等级保护密码技术要求”四标准制修订	国家密码管理局	主要参与单位
11	《个人信息保护技术指引》制定	中国支付清算协会	主要编写单位
12	《条码支付安全技术指引》意见征集	中国支付清算协会	主要编写单位
13	《电子招标投标系统技术规范》制定	中国招投标协会	主要编写单位

对外合作

2013年

- 与中国人民公安大学等八家单位共同成立“网络犯罪与信息安全协同创新中心”

2014年

- 由中国工程院沈昌祥院士提议，中国电子信息产业集团、中国信息安全研究院、北京工业大学、中国金融认证中心等60家单位发起，成立“中关村可信计算产业联盟”

2015年

- 百度、腾讯、中国科学院信息工程研究所、上海交通大学信息安全工程学院，联合成立“**移动金融安全研究联合实验室**”
- 腾讯、CFCA信息安全实验室、中国标准化研究院联合举办“第一届互联网安全领袖峰会（CSS）”

目　录

目　录

用户个人数据泄露与非授权使用

美国选民登记信息被贩售

2016年7月，据外媒报道，黑客在暗网大肆贩卖美国大选选民的登记数据。
暗网出现了一位声称拥有全部美国大选的选民登记记录数据，并且还可提供选民的具体州属，贩卖的价格定为**每州的数据340.38美元**。
同时，据报道，早在2015年12月，一位安全研究员即发现有**1.91亿美国选民登记数据**在网上流传

Yahoo5亿用户邮箱信息2年前被盗

泄露的信息包括：**用户姓名、电子邮件地址、电话号码和哈希密码**
2016年8月，据外媒报道
雅虎发现匿名黑客销售含有2亿个雅虎账户登录信息的数据库。经查，这些数据源自于2014年底，作为最早的邮件服务提供商，预计总体被盗用户信息约为5亿。

美国富国银行内部员工违规使用用户个人数据

2016年9月，
因内部员工违规使用用户个人数据，富国银行接收由联邦消费者金融保护局（federal Consumer Financial Protection Bureau）、货币监理检察官办公室（the Office of the Comptroller of the Currency）和洛杉矶市的相关部门联合**处罚1.85亿美元**。同时富国银行**需向客户支付约为500万美元的损失与补偿**。
事由：内部员工非授权使用客户信息或通过虚假诱导开设超过150万个储蓄账户，并把现有账户内的钱转至新设账户。
在客户不知情或未同意的情况下申请超过56万个信用卡账户。

目　录

个人数据是指？

不同地域、行业有不同的界定与要求

美国

《隐私权法》（Privacy Act）

个人记录是指“**行政机关根据公民的姓名或其他标识而记载的一项或一组信息**”。其中，“其他标识”包括别名、相片、指纹、音纹、社会保障号码、护照号码、汽车执照号码，以及其他一切**能够用于识别某一特定个人的标识**。个人记录涉及教育、经济活动、医疗史、工作履历以及其他一切关于个人情况的记载。

——《隐私权法》（Privacy Act）

欧盟

《数据保护指令》第2(a)条

“个人数据是指，**与一个身份已被识别或者可被识别的自然人相关的任何信息**；**身份可被识别的人**是指，其身份可以直接或者间接，特别是通过身份证号码或者一个或多个与其身体、生理、精神、经济、文化或社会身份有关的**特殊因素来确认的人**。”

——1995 年《关于与个人数据处理相关的个人数据保护及此类数据自由流动的指令》即《个人数据保护指令》第2(a)条

日本

《个人信息保护法》第2条

“所谓个人信息就是指**有关活着的个人的信息**，根据该信息所含有姓名、出生年月以及其他一些描述，能把该个人从他人中识别出来的与该个人相关的信息（包含能简单的查对其他的信息，根据那些信息来识别个人的东西）。**由这些个人信息组成的集合物形成个人信息数据库**。”

——《个人信息保护法》第2条 2003年获批，2005年实施

个人数据是指？（续）

我国有关标准对于个人信息的一些界定

个人信息

个人信息 personal information
可**为信息系统所处理**、与特定自然人相关、能够单独或通过与其他信息结合**识别该特定自然人的计算机数据**。
个人信息可以分为个人敏感信息和个人一般信息。

个人敏感信息

个人敏感信息 personal sensitive information
一旦遭到泄露或修改，会对标识的个人信息**主体造成不良影响的个人信息**。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。

个人一般信息

个人一般信息 personal general information
除个人敏感信息以外的个人信息。

——GB/Z 28828-2012 《信息安全技术 公共及商用服务信息系统个人信息保护指南》

个人数据是指？（续）

我国金融行业的一些说明

个人金融信息

个人金融信息
是指银行业金融机构在**开展业务时**，或**通过接入中国人民银行征信系统、支付系统以及其他系统获取、加工和保存的**以下**个人信息**：
（一）个人身份信息、（二）个人财产信息、（三）个人账户信息、（四）个人信用信息、（五）个人金融交易信息、（六）衍生信息、（七）在与个人建立业务关系过程中获取、保存的其他个人信息。

——银发〔2011〕17号《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》

支付敏感信息

支付敏感信息
包括：银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等。

——银发〔2016〕170号文《中国人民银行关于进一步加强银行卡风险管理的通知》

目　录

目　录

美国的个人数据保护

强调隐私权。围绕隐私权法，在敏感领域分散立法。

隐私权法（ Privacy Act）

1974年参众两院审议通过，1979年编入美国法典。
美国保护隐私权的基本法

儿童在线隐私权保护法

Children's Online Privacy Protection Act

财务隐私法

The Right to Financial Privacy Act

有线通讯隐私权法案、电子通讯法案

The Electronic Communication Privacy Act

等等.....

美国的个人数据保护（续）

不同与隐私权法，对于信息化的人信息保护的具体措施，采取行业自律模式。既要保护个人隐私，又不希望切断信息的自由流动。

个人隐私和国家信息基础设施：个人信息的使用和提供原则

1995年，美国政府信息基础设施特别工作组（IITF）下设的个人隐私工作组
提出了有关个人**信息收集、加工、处理、再利用**的基本原则。

TRUSTe

对信息化的个人数据进行隐私评估与认证的机构，服务范围包括：

- All Your Websites, Mobile Apps, and Cloud Platforms
- Online and Offline Data Sources
- Customer, Partner, and Employee / HR Data Sources
- Global Coverage – North America, South America, EMEA, Asia, Australia, etc.
- Cross Border Data Transfers
- Data Processor and Data Controller Relationships

全球电子商务政策框架

A Framework For Global Electronic Commerce

克林顿政府1997年发布
强调私营企业在保护网络隐私权中的主导作用，
支持私营企业为此进行的**自我规范**的努力。

美国的个人数据保护（续）

安全港协议

2000年，美国政府与欧盟就实现个人信息**跨境自由流动**协商的个人信息保护原则。

美国企业自愿参加。

2015年，因众所周知的原因被欧盟最好法院宣布无效。

全球”大数据”白皮书《大数据：把握机遇，守护价值》

2014年5月，美国总统执行办公室提出了**收集主体告知义务难以有效监测**、**行为人难以控制自己的数据应用情境**、原有数据储存方式受到挑战，**数据泄露风险增大**、**大数据资源公开与共享诉求与隐私权相矛盾**等问题。

白皮书认为，大数据时代的隐私保护**应当关注于使用责任制**，数据的采集者和使用者对数据的管理及其可能产生的危害负责。同时，美国政府对隐私保护政策框架**持较为开放的态度。**

网络环境下消费者数据的隐私保护–在全球数字经济背景下保护隐私和促进创新的政策框架

2012年，美国总统奥巴马签署美国白宫发布的工作报告。正式提出《消费者隐私权利法案》（Consumer Privacy Bill of Rights）

强化“告知与同意”框架、提出**数据保存与处理的安全责任**、明确**事后问责制**

欧盟的个人数据保护

由国家主导的立法模式。欧盟统一立法和欧盟成员国国内立法的两层模式。

保护自动化处理个人数据公约

Council of Europe：Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

1980年欧共体时代，通过了《保护自动化处理个人数据公约》。当时的欧洲议会为在各成员国间保护经自动化处理的个人数据。

关于与个人数据处理相关的个人数据保护及此类数据自由流动的指令

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

1995年,欧洲联盟通过了《个人数据保护指令》。包括**个人数据处理形式、个人数据收集、记录、储存、修改、使用或销毁，以及基于网络的个人数据收集、记录、传播**等，规定欧盟各成员国必须根据这个指令，制定本国的个人数据保护法，以保障个人数据资料在成员国间的自由流动。

欧盟的个人数据保护

一系列法案、指令、原则、准则、指南等

《电子通讯数据保护指令》、《私有数据保密法》、《互联网上个人隐私权保护的一般原则》、《关于互联网上软件、硬件进行的不可见的和自动化的个人数据处理的建议》、《信息公路上个人数据收集、处理过程中个人权利保护指南》等

通用数据保护条例

General Data Protection Regulation，**GDPR**

2016年4月，通过，2018年5月25日正式生效。

对于成立地在欧盟内的机构，强调无论数据处理的活动是否发生在欧盟经理，都统一遵循条例。

对于成立地在欧盟以外的机构，使用署人原则。只要提供的产品或服务（不论是否收费）处理了欧洲境内个体的个人数据，将同样适用与《条例》。

敏感数据中明确加入了基因数据、**生物数据**。

关于数据画像（profiling）：数据主题明确同意；欧盟成员国法律明确授权；数据主体和数据控制着之间签订协议。3者均满足要求才可提供服务

对于**个人敏感数据的数据画像活动是被禁止的。除非获得了数据主体出于一个或多个目的同意。**但成员国可通过立法明确禁止；**或该数据画像对于重大公共利益是必须的。**

日本的个人数据保护

立法与行业自律相结合

立法

- **《个人信息保护法》**（個人情報の保護に関する法律）
  2003年通过，2005年实施，为日本国内有关领域基本法。
  包括总则（目的和基本理念）、国家和地方公共团体的责任和义务、个人信息保护方针和政策、个人信息处理业者的责任、法律例外和处罚。

- 其他系列国家行政机关、地方公共团体、行政法人等的相关法规。

行业自律

P-MARK认证（The Privacy Mark System）
日本工业标准（JIS）《个人信息保护管理体系要求事项》（JIS Q 15001）
是参考ISO/IEC 27001细化的个人信息保护体系要求，为日本可操作的行业自律标准，包含以下内容：

- 个人信息保护方针
- 风险分析和风险管理措施
- 管理规章
- 个人信息保护管理体系实施的监察
- 个人信息保护管理体系文档管理
- 个人信息收集、利用、提供的例外等

国际上的标准化工作

国际标准

ISO/IEC JTC1/SC27/WG5工作组 Identity management and privacy technologies

ISO/IEC 29100系列标准：

- ISO/IEC 29100《隐私保护框架》：隐私框架的基本要素、隐私遵守的原则
- ISO/IEC 29101《隐私体系架构》：对设计和维护系统处理PII的系统具有指导意义
- ISO/IEC 29190《隐私能力评估模型》
- ISO/IEC 29134《隐私影响评估》
- ISO/IEC 29151《个人可识别信息保护指南》：PII（个人可识别）安全控制措施和风险处理指南

美国国家标准与有关出版物

NIST SP 800系列：

SP 800 -53v4《联邦信息系统和组织的安全与隐私控制》
Security and Privacy Controls for Federal Information Systems and Organizations

SP 800-122《保护个人可标识信息（PII）保密性指南》
Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

SP 800-144《公共云计算安全和隐私保护指南》
Guidelines on Security and Privacy in Public Cloud Computing

NIST出版的联合工作报告NISTIR 8062《联邦信息系统隐私风险管理》
Privacy Risk Management for Federal Information Systems

国际上的标准化工作

欧盟

数据保护和隐私工作组（CEN/ISSS WS-DPP）：

CWA 16113:2010《个人数据保护良好实践》、

CWA 15263:2005《隐私保护技术、隐私增强技术（PET）、隐私实践体系（PMS）和身份管理系统（IMS），及上述方面的驱动者和标准化需求分析》、

CWA 16112:2010《管理者的自评估框架》、

CWA 15292:2005《协助遵守数据保护指令95/46/EC的第17条所规定义务的标准格式合同》、

CWA 15262:2005《数据保护审计实践清单》

目　录

我国的进展

网络安全法

《中华人民共和国网络安全法（草案二次审议稿）》，
2016-07-05 至 2016-08-04公开征求意见。

公民个人信息

第七章　附则 第七十二条 第五款：
公民个人信息，是指以**电子或者其他方式记录**的**能够单独或者与其他信息结合识别公民个人身份的各种信息，**包括但不限于公民的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。“

——中国人大网，“网络安全立法”专题
http://www.npc.gov.cn/npc/lfzt/rlyw/node_27975.htm

我国的进展

网络安全法（草案）

第二十一条 、第四十条至第四十五条：

- 对**收集、使用**提出要求，
- 明确“**网络运营者不得泄露、篡改、损毁其收集的公民个人信息**；
- **未经被收集者同意**，不得向他人提供公民个人信息。
- ”网络运营者**应当采取技术措施和其他必要措施，确保公民个人信息安全**，防止其收集的公民个人信息泄露、毁损、丢失。”
- **发生**公民个人信息泄露、损毁、丢失的**事件**时，**应采取补救措施，并履行告知与通报义务**。
- 对于公民个人信息属主，**公民有权要求违法违规使用方删除其个人信息**，并发现其个人信息**有误时，有权要求运营者予以更正**。
- “任何个人和组织**不得窃取或者以其他非法方式获取公民个人信息，不得非法出售或者非法向他人提供**公民个人信息”

“第六章 法律责任 ”中对违法违规使用公民个人信息的情况提出了惩罚性要求

在草案第二次审议稿中“增加大数据应用必须**对公民个人信息进行无法识别特定个人处理的规定**，进一步明确公民个人信息使用规则（草案二次审议稿第四十一条第一款）”

——中国人大网，“网络安全立法”专题
http://www.npc.gov.cn/npc/lfzt/rlyw/node_27975.htm

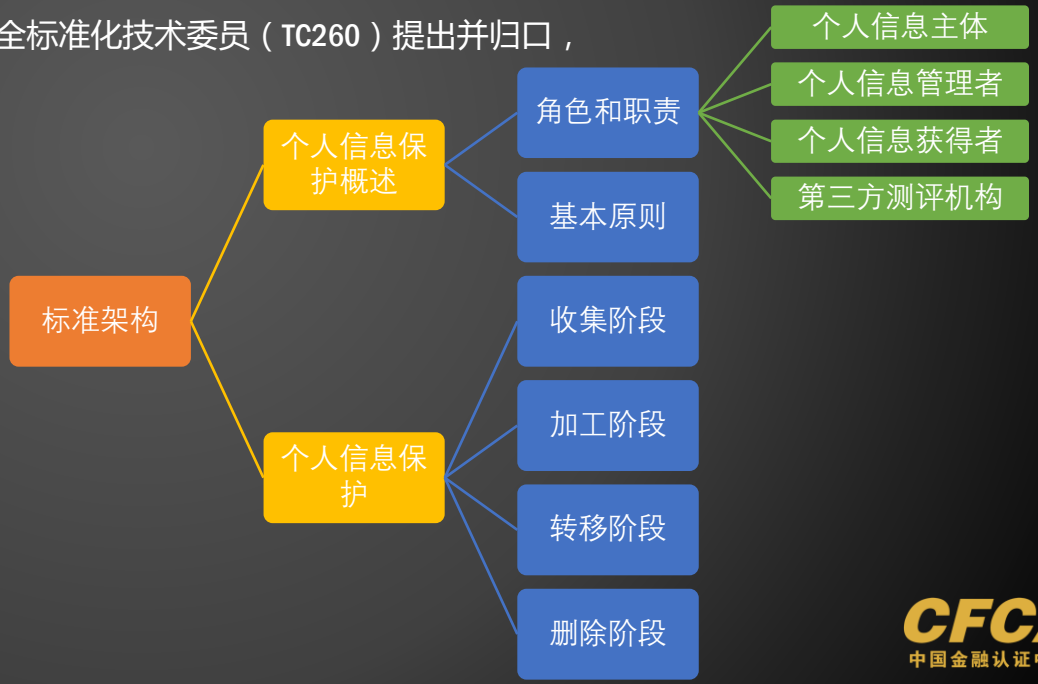
我国的进展：标准

国家标准

GB/Z 28828-2012 《信息安全技术 公共及商用服务信息系统个人信息保护指南》

中国首个个人信息保护国家标准，于全国信息安全标准化技术委员（TC260）提出并归口，2013年2月1日起实施。

- 个人信息分为**个人一般信息**和**个人敏感信息**
- 提出**默许同意**和**明示同意**的概念：对于个人一般信息的处理可以建立在默许同意的基础上，只要个人信息主体没有明确表示反对，便可收集和利用。**对于个人敏感信息，则需要建立在明示同意的基础上，在收集和利用之前，必须首先获得个人信息主体明确的授权**。
- 处理个人信息时应当遵循的**八项基本原则**，即**目的明确、最少够用、公开告知、个人同意、质量保证、安全保障、诚信履行和责任明确**
- 提炼个人信息处理的**4个阶段**



我国的进展：标准

国家标准（续）

《信息安全技术 公共及商用服务信息系统个人信息保护指南》（补篇）

GB/Z 28828-2012 对于具体技术要求的补充，于全国信息安全标准化技术委员（TC260）WG7工作组立项，目前为在研标准。

- 在GB/Z 28828-2012 基础上增加章节6“信息系统个人信息保护技术要求”
- 从个人信息保护安全功能要、个人信息处理过程安全保证两部分，提出具体的，具有操作实施指导性的技术要求

《信息安全技术 信息系统个人信息保护管理要求》

个人信息保护标准体系包括基础类、技术类、管理类和应用类标准，此标准为管理标准。
于全国信息安全标准化技术委员（TC260）WG7工作组立项，目前为在研标准。

- 目前草案框架如下：
  - 策略与制度
  - 机构与人员
  - 环境与资质
  - 操作与维护
  - 个人信息处理
  - 风险控制

我国的进展：金融行业

金融行业政策与标准化情况

银发〔2011〕17号 《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》

- 提出个人金融信息的概念
  1. 个人身份信息
  2. 个人财产信息、
  3. 个人账户信息
  4. 个人信用信息、
  5. 个人金融交易信息、
  6. 衍生信息、
  7. 在与个人建立业务关系过程中获取、保存的其他个人信息。
- 明确信息保护的基本要求：
  - 银行业金融机构在**收集、保存、使用、对外提供**个人金融信息时，应当严格遵守法律规定，采取有效措施加强对个人金融信息保护，确保信息安全，防止信息泄露和滥用
  - **建立健全内部控制制度**
  - **完善信息安全技术防范措施**
  - **境内采集的个人信息存储**
  - **外包服务的控制等**
- 不得篡改、违法使用个人金融信息，明确不正当使用个人金融信息的几种情况
- 明确个人金融信息泄露的报送机制与惩戒措施

我国的进展：金融行业

金融行业政策与标准化情况

（银发〔2016〕170号文）《中国人民银行关于进一步加强银行卡风险管理的通知》

- 提出支付敏感信息
  1. 银行卡磁道或芯片信息、
  2. 卡片验证码、
  3. 卡片有效期、
  4. 银行卡密码、
  5. 网络支付交易密码等

- 明确处理支付敏感信息的机构主体
  1. 商业银行、
  2. 支付机构（从事银行卡收单、网络支付业务的非银行支付机构）

- 对支付敏感信息的管理提出内控要求
- 从技术角度提出对支付敏感信息的处理要求

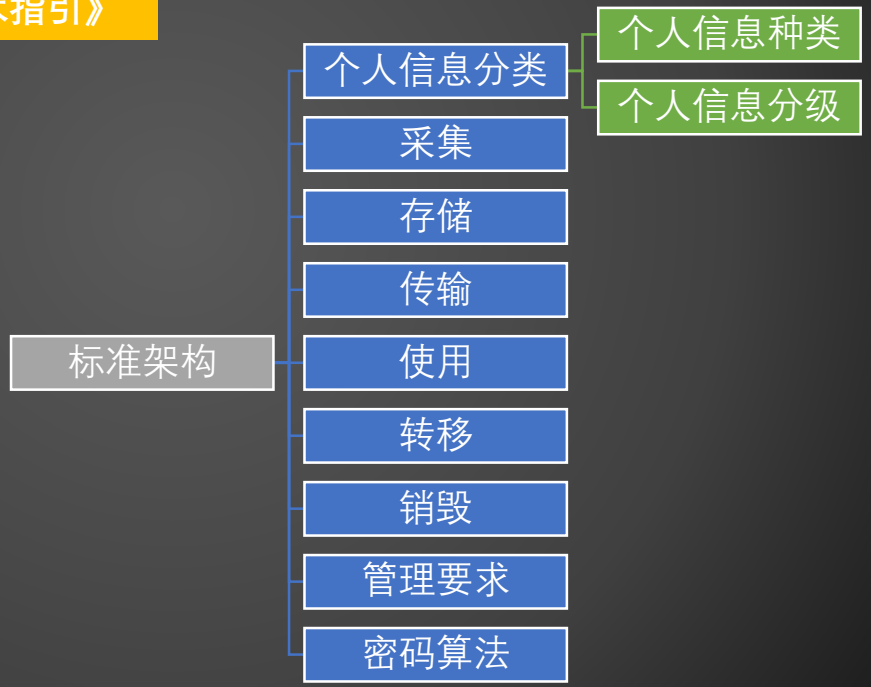
我国的进展：金融行业

金融行业政策与标准化情况：行业自律

PCACT 0001-2016《个人信息保护技术指引》

由中国支付清算协会技术标准工作委员会发布，金融行业行业协会关于个人信息保护的行业自律规程，
给出了信息系统处理个人信息的范围定义，
界定个人信息主体的权利，
提出了 系统处理个人信息的原则和个人信息的采集、展示、存储、传输、使用等行为要求。

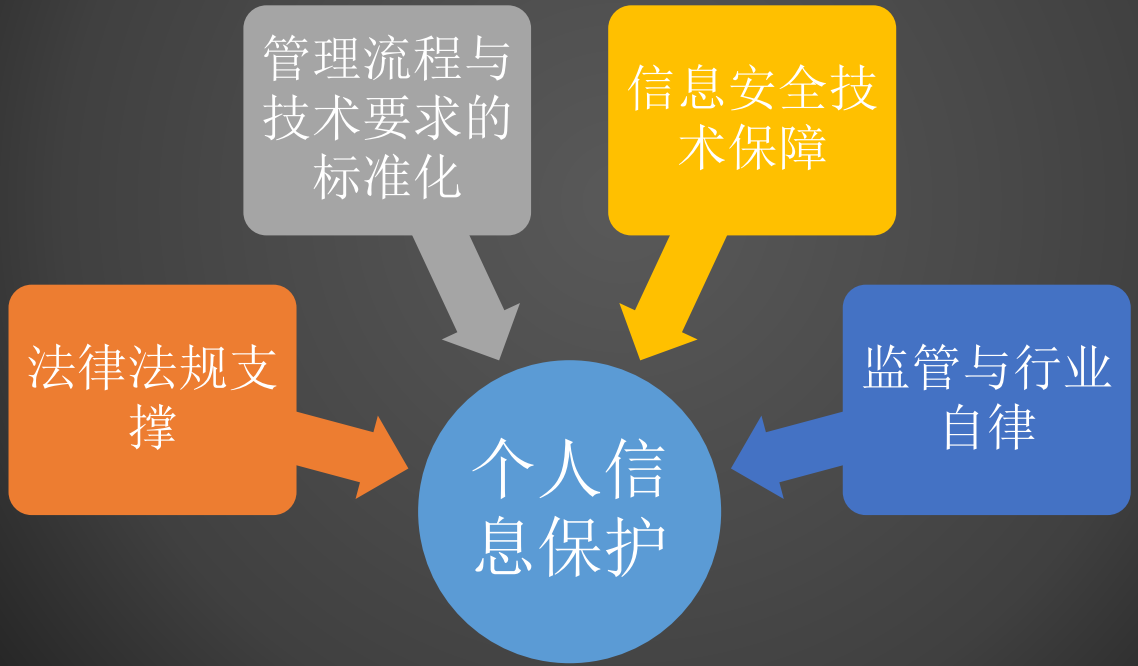
用于指导本协会会员单位利用信息系统处理个人信息的服务与活动



目　录

我国的进展：金融行业

关于个人数据的保护，尤其是金融数据的保护，我们一直在路上。



参考与引用

除本幻灯片标识中有关国内外引用法律、标准外，还包括：

《各国个人信息保护情况》来源：chinapipa 163 blog

《个人信息保护标准综述》作者：洪延青 左晓栋，《信息技术与标准化》 2016年06期

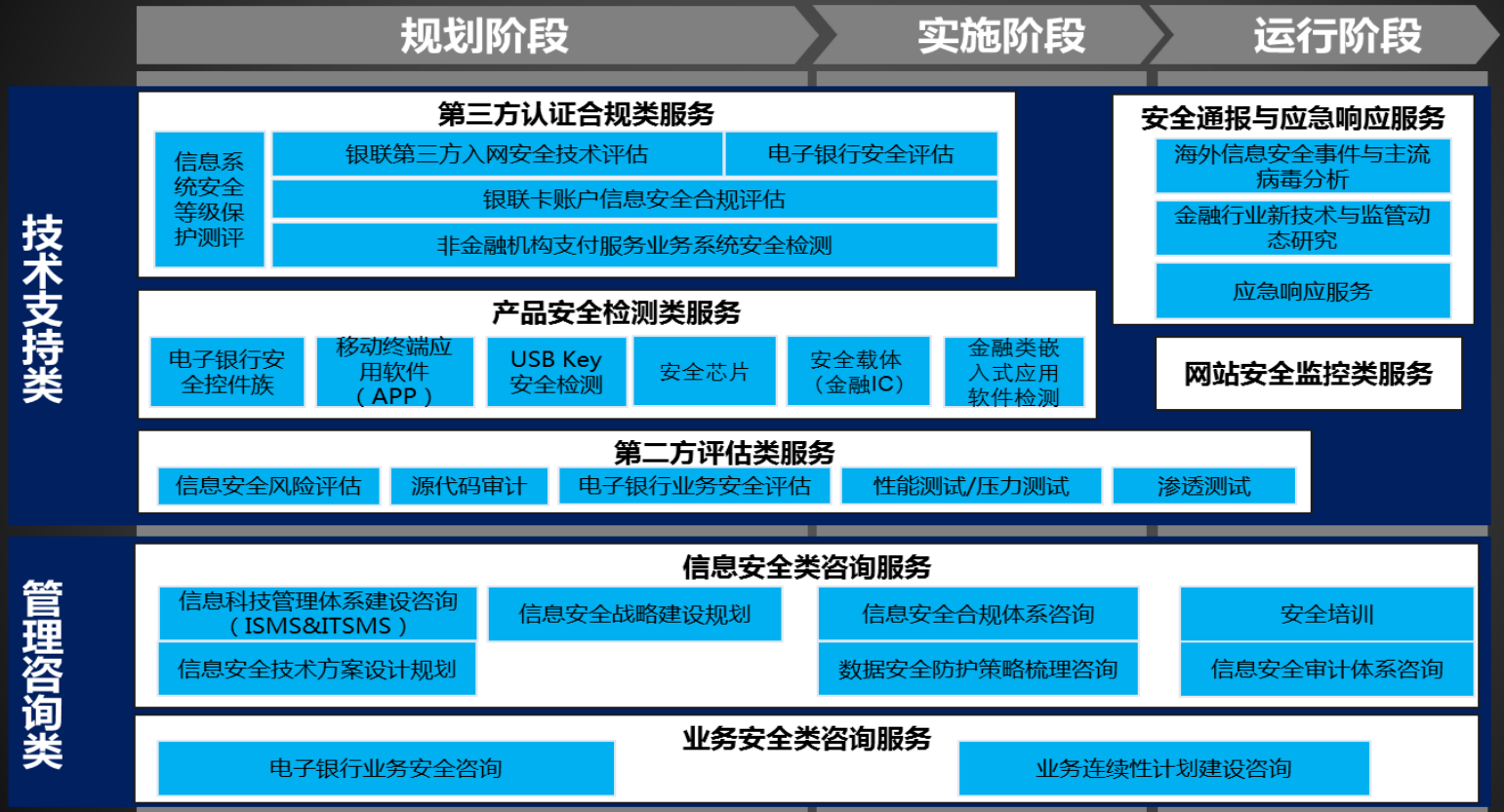
“大数据时代”的美国隐私权保护制度 作者：李明，北京大学金融法研究中心

《日本的个人信息保护法制及启示》作者：谢青，《政治与法律》，2006年06期

欧盟《通用数据保护条例》详解，作者：王融，《大数据》，2016年04期

那么最后……

CFCA信息安全实验室信息安全服务目录



谢　谢

CFCA
中国金融认证中心