CAICT 中国信通院

大数据时代的数据安全挑战与管理

——“ITValue＋企业信息安全论坛”

谢 玮

2016年7月

Content 主要内容

1 大数据时代下的数据安全挑战

2 国内外数据安全立法与监管实践

3 对我国数据安全管理的启示

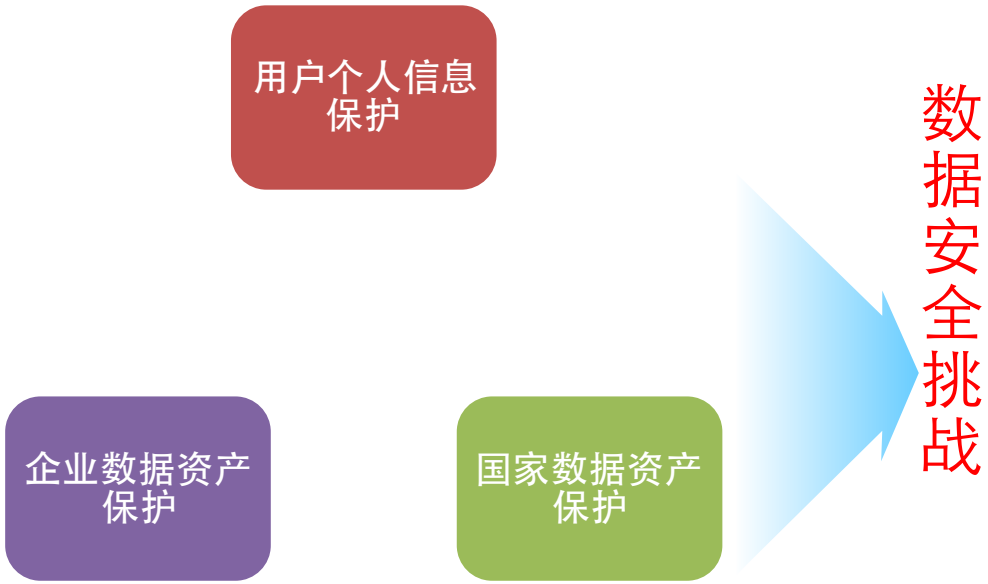
大数据时代下的数据安全挑战

大数据时代的三大特征

- **数据规模进入“PB”时代**：越来越多的企业生产生活、个人生活隐私被数字化和网络化，虚拟世界逐步成为物理世界的完整映射；
- **“无处不在”的数据采集**：可穿戴设备、车载设备、监控摄像探头、卫星遥感技术等，带来了更加丰富的数据来源；
- **超强的数据关联分析能力**：数据不断汇聚、融合，深度挖掘零散数据间的关系，实现更强决策、更深洞察。

大数据时代下的数据安全挑战

大数据时代，当我们谈论数据保护，我们想保护什么？



- 用户个人隐私受到严重威胁
- 国家间围绕数据资源的争夺日趋激烈
- 企业面对的数据安全威胁持续升级
- 数据安全管理面临挑战数据跨境流动安全
- ……

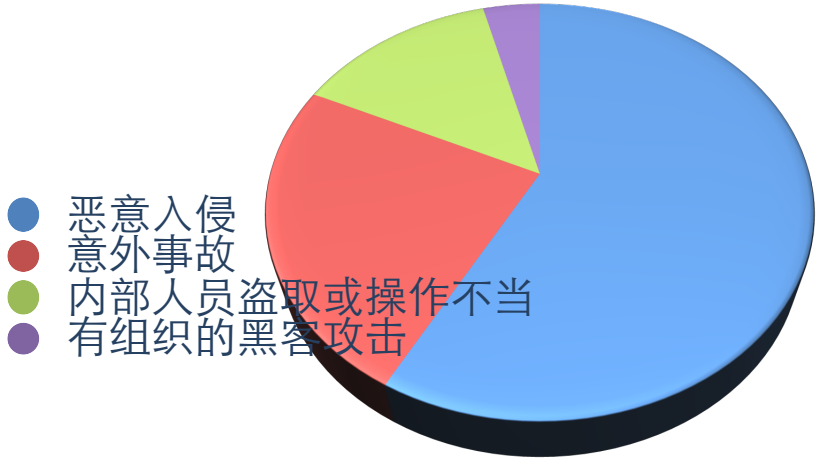
用户隐私数据泄露事件成倍增加，监管保护亟须加强

近年来，用户隐私数据泄露事件成倍增加，事件带来损失不断扩大，用户隐私信息保护已经成为全球各国网络空间安全监管的巨大难题。

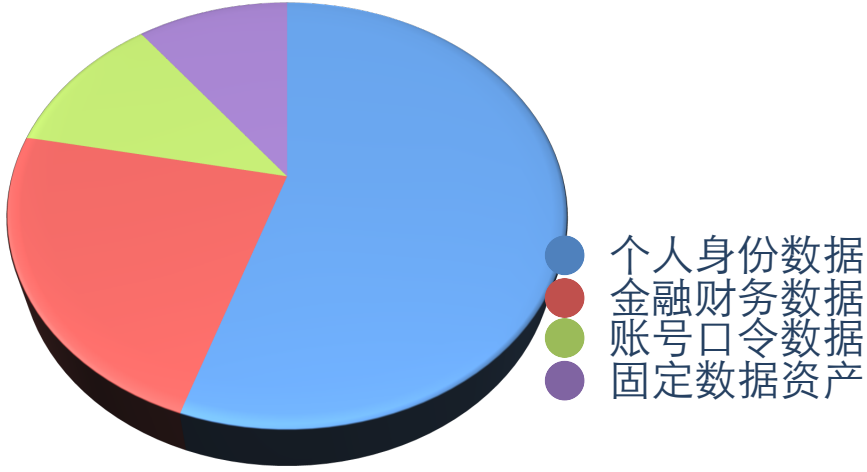
- 2015年，全球共发生**1673例**数据泄露事故，共造成 **7.07亿**条数据记录外泄。
  - **Ex.**2015年8月，大X网**600余万**用户账户密码遭到泄露和售卖
  - **Ex.**2015年5月，美国税局遭网络攻击泄露**10.4万**纳税人信息并损失**5000万**美元

数据来源：Gemalto

数据泄露威胁来源



泄露数据类型



新型网络攻击不断增加，企业现有保护手段难以抵御

近年来，ATP攻击与全球性高危漏洞事件时有发生，**新的网络攻击模式不断出现、攻击频率日趋密集、威胁范围不断扩大，大数据、云计算等新兴信息技术广泛应用引入新型数据安全威胁，**现有数据安全保护策略已无法有效应对。

针对企业数据资源的网络攻击不断增加

- 自2013年以来，数据中心遭遇**DDoS攻击**的占比已经达到了**70%**

- 2014年，索尼影音公司遭遇ATP攻击，硬盘数据被毁坏，大量员工信息及影视拷贝遭泄露。

新技术的融合应用易引发新的安全隐患

- 大数据、云计算技术带动信息系统软硬件架构的全新变革，可能在软件、硬件、协议等多方面**引入未知的漏洞隐患，现有数据安全保护技术“无能为力”。**

国际数据资源竞争博弈激烈，数据跨境流动成为关注点

随着数据资产战略价值不断攀升，数据跨境流动日趋频繁，各国对数据资源的**争夺逐步升级**，数据跨境流动**监管态度各异**，**难以形成全球统一规则。**

- 西方国家对数据资源已经进入“掠夺”时代
  - **Ex.**美“梯队”项目搜集全球**90%**通信信息
  - **Ex.**英“颞颥”项目监听**承担全球电话和网络流量**的光缆系统

- 数据跨境流动客观上加大了**国家关键数据资源流失的风险**
- “后棱镜”时代，国际网络互信氛围被打破，各国都担心自身**数据主权**的控制权能和保密权能受到侵害。

- 针对数据跨境流动问题，美国倡导基于“**数据共有，自由流动**”，与我国等倡导的“**数据主权**”理念有很大分歧。

国际间**数据资源流动需求与数据安全保护需求的矛盾已逐渐凸显，**如何开展监管，保卫数据主权，已成为各国都需解决的重要课题。

趋势变化

随着网络数据价值的不断增加，针对网络数据的安全威胁也与日俱增，给数据安全保障带来了严峻的挑战，使很多国家对网空数据的使用从“注重开放”转向“强调保护和治理”。

“棱镜门”事件前，数据开放是趋势，针对跨境流动等的国际合作不断推进。

注重开放 ➡ **强调保护**

各国开始明确并不断强化数据保护责任，网络数据成为重要的国家资源

Content 主要内容

1 大数据时代下的数据安全挑战

2 国内外数据安全立法与监管实践

3 对我国数据安全管理的启示

全球各国应对大数据时代安全挑战的立法举措

p 一个充满变革的时代：

- ❑ 欧盟即将实施**最为严格**的数据保护法规 …
- ❑ 美国用户隐私保护**监管执法**持续发力 …
- ❑ 中国用户个人信息保护法律框架**基本成型**，各行业监管部门正在制定互补的数据保护法规…

欧盟应对大数据时代安全挑战的立法举措

今年4月14日，欧盟通过《数据保护总规》（General Data Protection Regulation），2018年正式生效

基本原则

- 合法，公平，透明
- 目的限定
- 数据最小化
- 准确
- 有限留存
- 完整，机密
- 责任

数据权利

- 被遗忘权
- 更正权
- 限制处理权
- 数据可携权
- 数据获取权
- 信息知情权
- 知情同意权
- ……

企业义务

- 设立数据保护官的义务
- 泄露通知的义务
- 限制用户画像
- 限制随意跨境转移
- ……

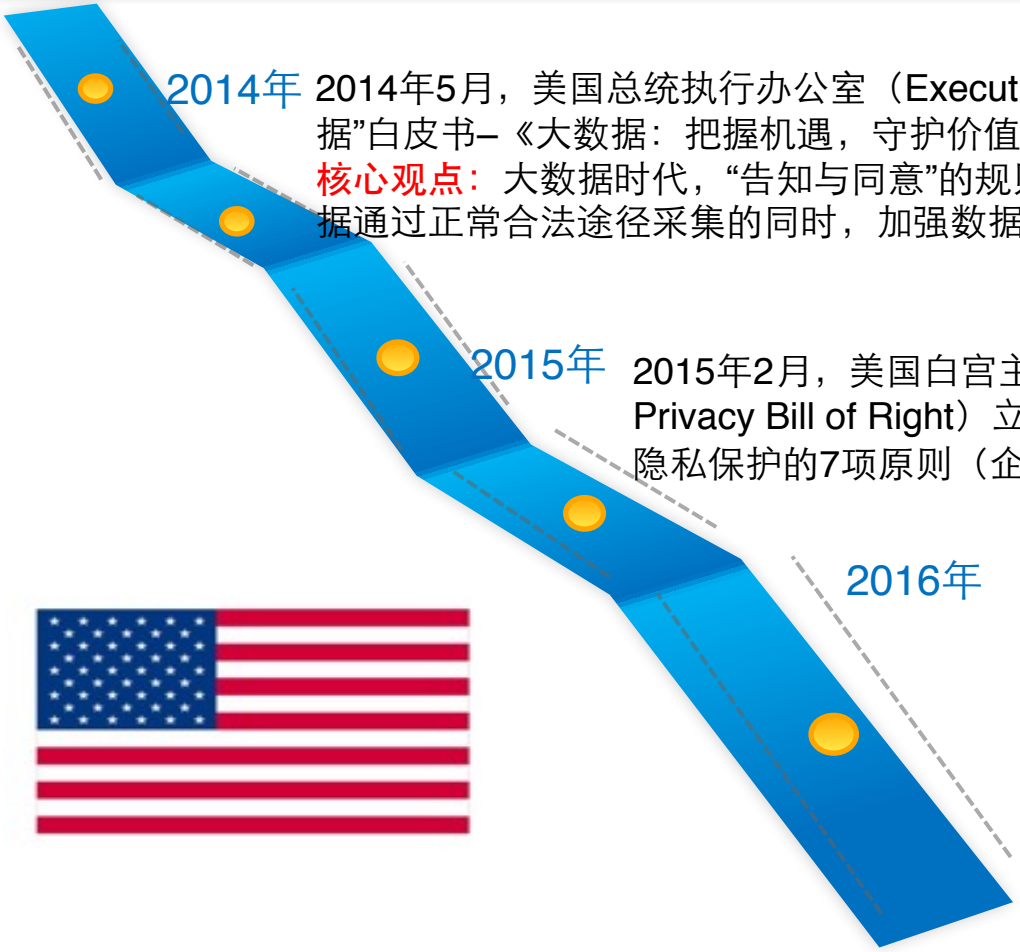
严格限制“数据画像”技术

——利用大数据技术处理个人数据的活动。

- 用户充分知情，且明确同意并授权
- 匿名化处理
- 分析结果禁止涉及儿童
- 分析结果不能导致对个人的歧视

欧盟的数据泄露通知制度与美国相比更为严格，要求企业在数据泄露事件发生后*24*小时内向外界通报。如果通知没有在*24*小时内完成，则应该解释延误原因。

美国应对大数据时代安全挑战的立法举措



2014年 2014年5月，美国总统执行办公室（Executive Office of the President）发布2014年全球“大数据”白皮书–《大数据：把握机遇，守护价值》BigData：Seize Opportunities, Preserving Values

核心观点：大数据时代，“告知与同意”的规则更容易被破坏，需要**重点关注使用**一端，确保数据通过正常合法途径采集的同时，加强数据开发利用过程的安全管理规则构建。

2015年 2015年2月，美国白宫主导的《消费者隐私权利法案》（Consumer Privacy Bill of Right）立法草案提交美国国会审议。草案中制定了消费者隐私保护的7项原则（企业责任），指定FTC作为监管部门加强执法。

2016年 **美国重新界定用户个人信息，尝试将IP 地址、设备标识纳入保护范围。**

2016年5月，叶尔绍夫（Yershov）起诉美国报业集团甘乃特（Gannett）案例中，美国联邦第一巡回法庭**判定设备标识结合地理位置信息能够关联到个人，应当视为个人可识别信息并予以保护。**此前联邦贸易委员会已在《儿童在线隐私保护规则》2013修订案中扩展了个人可识别信息的定义

各国针对数据跨境流动安全的立法尝试

- **数据跨境流动——涉及公民信息的数据应境内存储**
  - 俄罗斯2015年起实行新法，规定收集俄公民信息的互联网公司都应将这些数据存储在俄罗斯国内。
  - 欧盟最新通过的《数据保护总规（GDPR）》中规定：除非符合欧盟法律及相关国际条约或协定,**否则任何公司不得将欧盟公民的数据信息与欧盟之外的第三国分享**。
  - 2013年新加坡正式实施的《个人资料保护法令》明确规定机构不得将个人数据转移至境外除非依据本法的相关要求，确保机构能够提供符合本法要求的个人数据保护水平。
  - 巴西总统推进一项将巴西民众的信息储存在国内信息储存中心的法案，并建议铺设直通欧洲的海底光缆，免受美国监控。此法案一旦通过将会迫使谷歌等公司在巴西建立服务器。

各国针对数据安全的监管实践

- **数据安全调查和政府干预机制**
  - 随着数据侵权案件的飙升，美国联邦贸易委员会（FTC）加强了对不严格保护消费者信息安全的企业的调查。自2002起，FTC调查了许多公司的数据保护工作情况，**并对50多家公司采取了执法行动**，对涉事企业处以高额罚款并向社会公示。
    - 2012年美国谷歌公司因违反隐私保护规则被FTC判罚2250万美元，
    - 2014年GMR公司因泄露15,000份敏感个人信息（包括消费者的姓名、生日和医疗记录）被FTC提起数据安全执法诉讼。
  - 美国联邦通信委员会（FCC）规范互联网接入服务商收集、使用用户信息的行为
    - 2015年4月美国联邦通信委员会(FCC)针对美国第二大电信运营商AT&T数据泄露事件进行处罚。
  - 英德等国家也在法律中明确赋予**政府针对网络攻击的投诉进行调查**的权利。

中国应对大数据时代安全挑战的立法举措

- 我国尚未制定专门、统一的个人信息保护法；
- 现有立法对通过人格尊严、个人隐私、个人秘密、保障信息安全等实现对个人信息的直接或间接保护；
- 近年来各行业法律法规针对“个人信息保护”进行规定的趋势日渐明显。

效力层级	法律名称
法律	《刑法修正案》；《民法通则》；《侵权责任法》；《治安管理处罚法》；《全国人大关于加强网络信息保护的决定》；《全国人大常委会关于维护互联网安全的决定》
行政法规	《中华人民共和国电信条例》；《计算机信息系统安全保护条例》
部门规章	《互联网电子公告服务管理规定》；《规范互联网信息服务市场秩序若干规定》；《个人信用信息基础数据库管理暂行办法》；《计算机信息网络国际联网管理暂行规定实施办法》；《计算机信息网络国际联网安全保护管理办法》；《互联网电子邮件服务管理办法》；《互联网安全保护技术措施规定》；《规范互联网信息服务市场秩序若干规定》；《电信和互联网个人信息保护规定》
	金融、保险、医疗健康等行业在**数据本地化存储**、**数据跨境流动**等方面做出了行业内规定 电信和互联网行业正在制定适应**大数据发展需求**的**网络数据保护规则**

我国应对大数据时代安全挑战的立法举措

我国在用户个人信息保护方面基本上采用了“告知与同意”保护框架，但是法律规定过于原则，对如何**利用大数据对用户个人信息进行处理分析、数据共享合作过程中的用户个人信息保护**等问题缺少统一法律或规范性要求。

保护范围

“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”

——全国人大常务委员会《关于加强网络信息保护的决定》

基本原则

“应当遵循合法、正当、必要的原则”

——全国人大常务委员会《关于加强网络信息保护的决定》

具体规范

知情同意——明示收集、使用信息的目的、方式和范围，并经被收集者同意

禁止出售——不得出售或者非法向他人提供公民个人电子信息

……

处罚量刑

《刑七》引入“出售、非法提供公民个人信息罪”与“非法获取公民个人信息罪”；

《刑九》进一步加强了对个人信息违法行为的刑事责任追究。

Content 主要内容

1 大数据时代下的数据安全挑战

2 国内外数据安全立法与监管实践

3 对我国数据安全管理的启示

对我国数据安全保护管理的启示

为有效应对大数据时代针对数据安全的全新挑战，需要建立统一、完整的国家数据安全保护管理体系；企业应重点关注**用户个人信息保护、数据共享合作、数据跨境流动**等关键问题的安全管理。

p 加强用户个人信息保护

- **加强用户个人信息使用管理**
  - 对用户个人信息进行关联分析应仅限于提供服务的目的；
  - 脱敏后的用户个人信息应进行可恢复性评估；
  - 未脱敏的用户个人信息不应用于业务系统开发测试；
  - MAC、IP地址等可能涉及用户敏感信息的数据慎重使用
- **数据泄露通知机制**
  - 涉事主体在发生用户个人信息泄露事件后应通知受影响用户，提醒其采取防范措施。

p 加强数据共享合作管理

- **加强数据处理外包服务管理**
  - 防范外包服务人员违规获取数据；
- **加强对数据合作方的管理**
  - 签订安全协议；
  - 数据提供方应能够证明数据合作方对共享数据的保护水平不低于原有数据保护水平。

p 加强数据跨境流动监管

- **建立数据跨境流动数据安全评估机制**
  - 明确责任部门、评估流程、评估标准

结 语

数据规模化生产、分享、应用的时代已然来临，数据资源和公民信息的安全保障和治理已成为各国网络空间博弈的新焦点。

面对新形势新问题，坚持安全与开放并重，责任与发展兼顾，通过业界联合、政企联动等途径，共同完善网络空间安全保障体系，为国家数据资源和公民信息提供全方位的保护已成未来发展的共识和方向。

中国信息通信研究院

中国信息通信研究院（工信部电信研究院）始建于上世纪50年代，前身为邮电部邮电科学研究院。工业和信息化部电信研究院成立以来，深化改革，充分发挥综合优势，成为国家信息通信研究领域最重要的科研单位。围绕“政府智库、行业平台”的职责定位，秉承“厚德实学、兴业致远”的文化理念，与时俱进，开拓创新。

网络信息安全工作的定位与职责

- 立足信息通信（ICT）领域，围绕“网络空间可靠、可信、可管、可控”目标
- 坚持战略性、前瞻性和方向性研究，构建综合支撑平台和专业技术力量。

安全监管和法律法规支撑

国内外动态和战略研究

重大问题和专项研究

国家行业技术标准制定

安全监管支撑系统建设

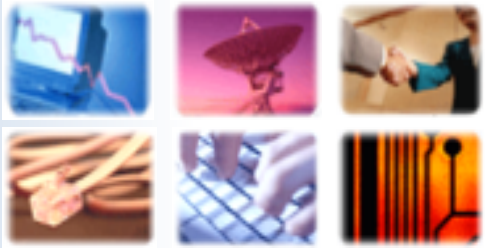
安全评估测试

安全试验验证

支撑政府安全管理
服务行业安全保障

CAICT 中国信息通信研究院
China Academy of Information and Communications Technology

感谢聆听
Thanks



谢玮
xiewei@caict.ac.cn