数据安全和1984

数据、安全和边界

关于我

- 任颂华（网名TR@SOE，肾上，老彼得爸），狗，宝瓶，第四代苏州人。
- 上海交通大学工学学士、硕士。
- 已婚，育有一子。
- 从事过园区开发、制造业、房地产等行业。
- 目前在苏州工业园区从事国际教育管理工作。

本书翻译历程

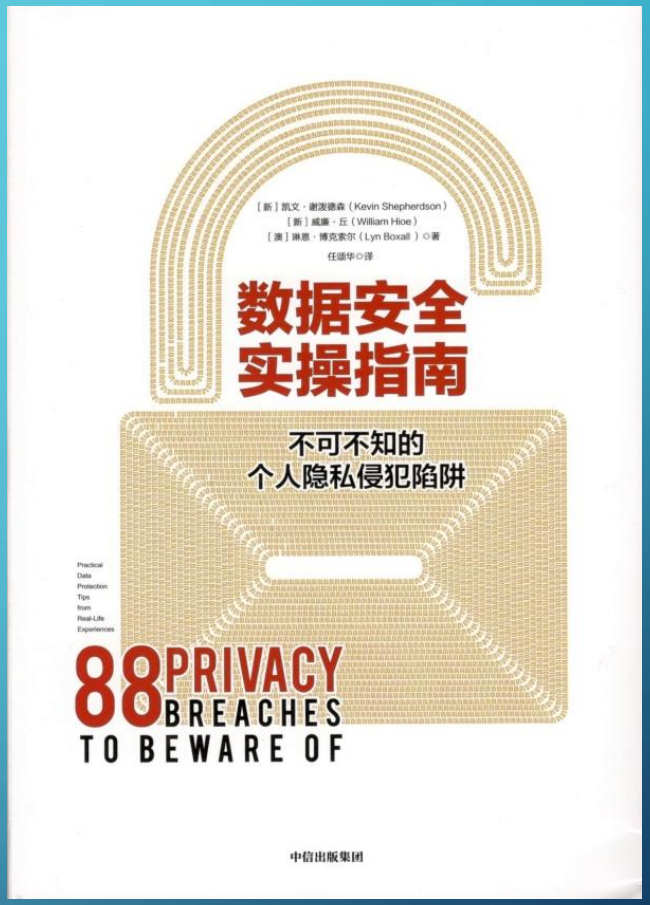
- 2017年01月20日，接到稿件，开始翻译。
- 2017年03月04日，签署翻译合同，谈好了周期和价格。
- 2017年03月24日，交稿。
- 2021年01月29日，新书到手——一本差点以为再也不会上架的译作。

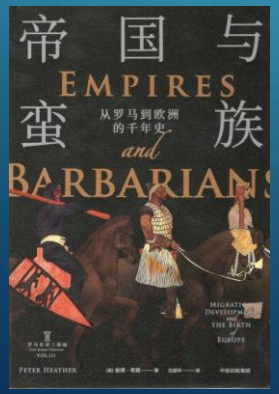
翻译过程中用到了多种工具，如：

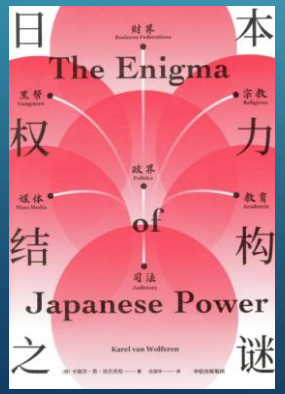
- Gitlab
- Google Translation
- Wiki

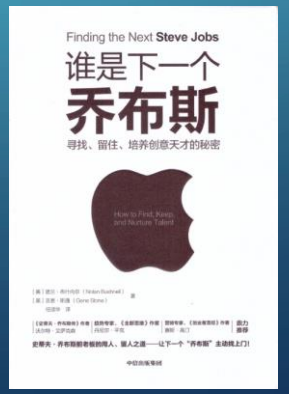
关于本书

- 个人翻译出版的第九本书
- 一本偏重“实操”多过“理论”探索的书
- 一本“能帮到你一些地方”的书
- 一本有趣的、接地气的、更能带来启发的书
- 一本可以随时带在手边的书









数据安全

- 数据安全，是指通过采取必要措施，保障数据得到有效保护和合法利用，并持续处于安全状态的能力。

Infringements upon Chinese netizens' rights and interests cost them 91.5 billion yuan ($13.8 billion) last year, according to a survey released at the China Internet Conference on Tuesday. - http://www.chinadaily.com.cn/business/2016-06/24/content_25841504.htm

频频接到金融推销，个人信息怎么泄露的？

- “消费贷款需要吗？利率低、还款方式灵活”“我们刚推出的一款保险产品很适合您”……上海市民李先生近期因为频频接到这类推销电话而烦恼：“对方张口就能说出我的身份证号、银行卡号等信息，甚至还知道我手头的资金状况，真不知道到底是哪个环节出了问题！”

https://news.sina.com.cn/c/2021-02-08/doc-ikftssap4712873.shtml

目前全球已有约90个国家和地区制定了个人信息保护法，而中国的《中华人民共和国数据安全法（草案）》已于2020年7月公开征求大众的意见。所有的公司和个人都将或早或晚地面对数据保护法，并把遵守数据保护法当作日常生活和工作的一部分。

欧盟、美国和中国的立法

- 1970年代，欧盟和美国都出现了数据保护的相关法规。
- 美国：Minimalist Approach. 相关约束散布在各种法律条文中，适用范围非常有限。数据隐私条款受限于言论自由的宪法要求。
- 欧盟：目标是设定涉及所有数据隐私事项的法令。2018年，GDPR（General Data Protection Regulation）成为所有成员国必须遵守的法律。
- 中国：有人认为，中国的文化传统是缺乏隐私保护的原因。

中国隐私保护立法简史

- 1982宪法，第40条： 中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。
- 1986年，《民法通则》101条：公民、法人享有名誉权，公民的人格尊严受法律保护，禁止用侮辱、诽谤等方式损害公民、法人的名誉。
- 2009年2月28日，《刑法修正案》（七）：在刑法第二百五十三条后增加一条，作为第二百五十三条之一：“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。……”
- 2012年12月，人大常委会关于加强网络信息保护的决定。中国更多采用了美国的做法，相关法律散布于银行、金融、消费者保护、邮政、医疗健康、信用征询、通讯和互联网等领域。（如，2013年，人大常委会更新了《消费者权益保护法》，其中第14条规定：消费者在购买、使用商品和接受服务时，享有人格尊严、民族风俗习惯得到尊重的权利，享有个人信息依法得到保护的权利。）

中国隐私保护立法简史（续）

- 2017年6月1日，《网络安全法》实施。
- 2018年5月1日，《GB/T 35273-2017信息安全技术 个人信息安全》生效。
- 2020年10月，《个人信息保护法》草案。
- 2021年1月1日，《民法典》生效。首次规定了隐私权和个人信息的保护原则，界定了个人信息的概念，列明了处理个人信息的合法基础，规范了个人信息处理者的义务、自然人对其个人信息的权利以及行政机关的职责。尽管存在诸多问题有待在未来的《个人信息保护法》中予以解决，但《民法典》为该领域的未来立法奠定了基础。隐私权第一次上升到“人格权”。

立法特色

- 对数据采集和处理的要求低。只有明确写出“需明确同意”时，才需要明确同意。
- 数据泄露的通知时间长。欧盟的72小时内 vs “及时”。
- 监管机构分散

- 立法一体化
- 对进一步处理的限制
- 最小的数据量
- 敏感数据（但没有明确列出）
- 遗忘权（美国认为这是对言论自由的侵犯(*)；中国在2016年5月有否定遗忘权的先行案例）
- 数据迁移
- 决策自动化和分析

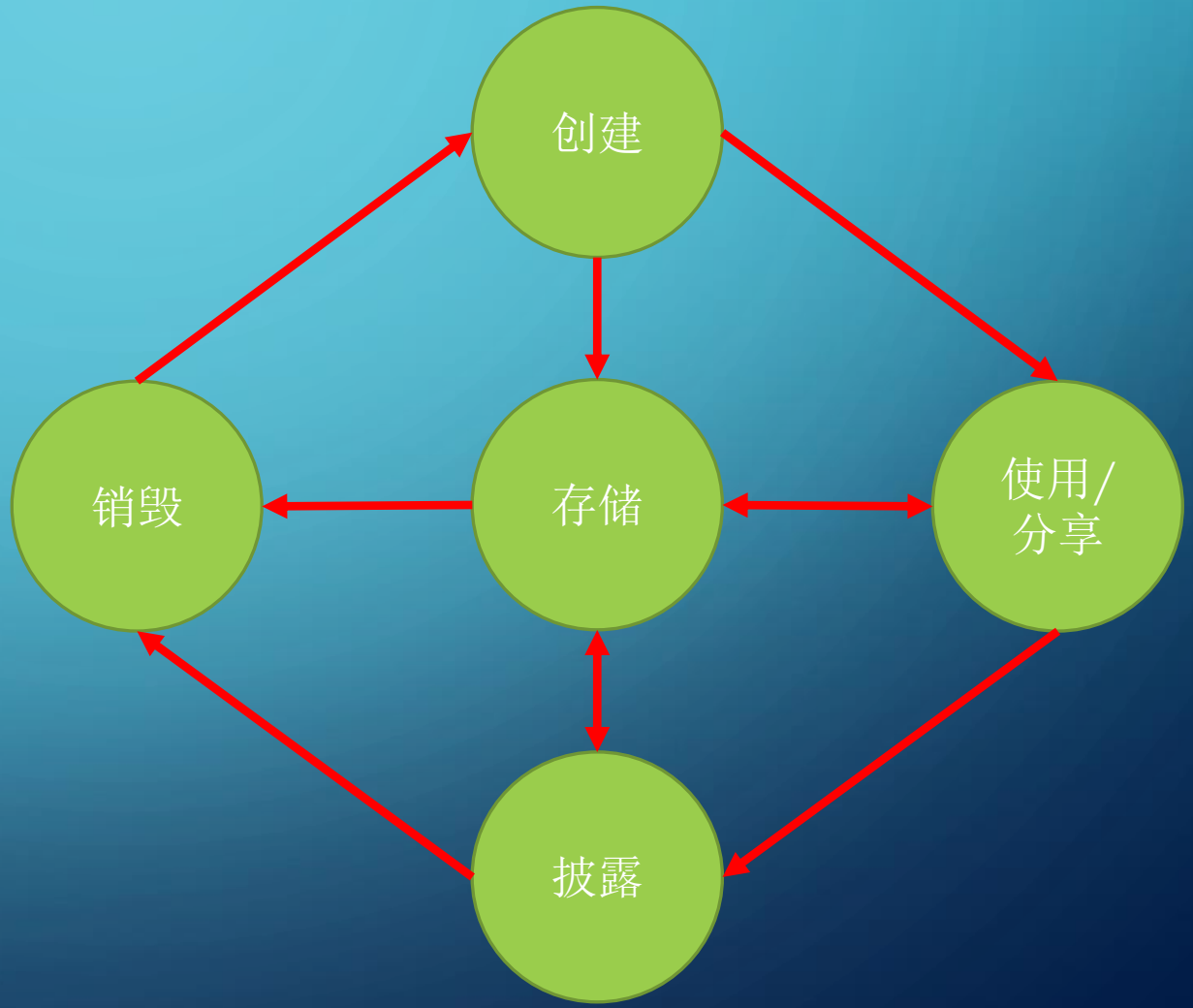
- https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos
- https://www.sohu.com/a/289881758_733746

中国特色

- 数据本地化和跨境数据传输
- 监控和隐私
- 消费者对数字经济的信心要增强；同时，
- 政府将成为隐私保护者

文件的生命周期

我曾经为一家公司担任顾问两年时间。在检查其合同存档的时候，发现最早的一个合同是7年之前的。而当前有效的合同就随意地放在销售的桌上，任何人都可以翻阅。其电子档放在网络盘上，授权名单中有早就离职的员工用户名，且每人都可以进行修改。



X象笔记的奇怪请求

- X象笔记在安装后并首次启动时，会要求“访问本网络中的设备”的权限。

必要性

Privacy By Design

0投诉=没有问题？

- 如今，要在网站上找到一个投诉入口实在是很难。最多就是一个“联系我们”的链接，但往往也不能直截了当地解决问题。

1. 投诉一定要简单
2. 员工清楚谁处理投诉
3. 尽快处理
4. 内部流程合理
5. 有升级路径
6. 及时反馈

我孩子在学校的照片应该如何使用？

- 某些学校（特别是国际学校）会在入学协议中规定：家长明确同意，学校可以在其站点和宣传渠道中使用学校活动中摄录的照片和视频。

1. 学校属于“非公开场合”。声明并获得家长（监护人）的同意是明智的，且这样的使用仅限于学校本身的教学、宣传活动。
2. 但如果不包括一个“撤回”的渠道，也是不完整的。
3. 学校的网站等也应采取必要的技术手段，防止搜索引擎搜索抓图并缓存，而使得图片“超出”了学校范围。

访客登记表和开放办公室

访 客 登 记 表										
序号	日期	时间	姓名	性别	单位	联系方式	内容摘要	所访人	接待人	备注
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										

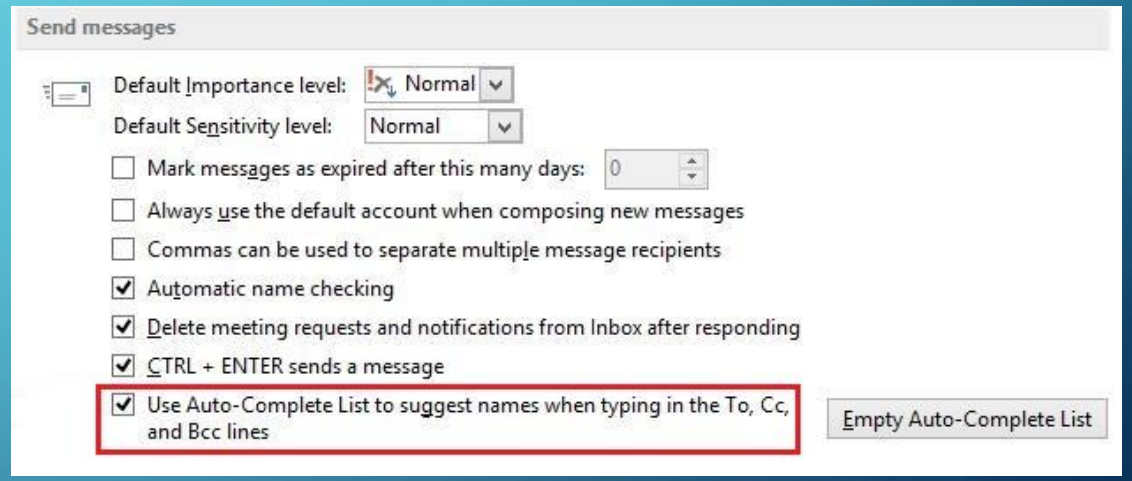
1. 所有后来的人都能看到有谁在之前来到；
2. 以及这些人的私有信息（电话、乃至身份证号码）；
3. 能不能有更隐私的方法？

我可以联系我的前客户吗？

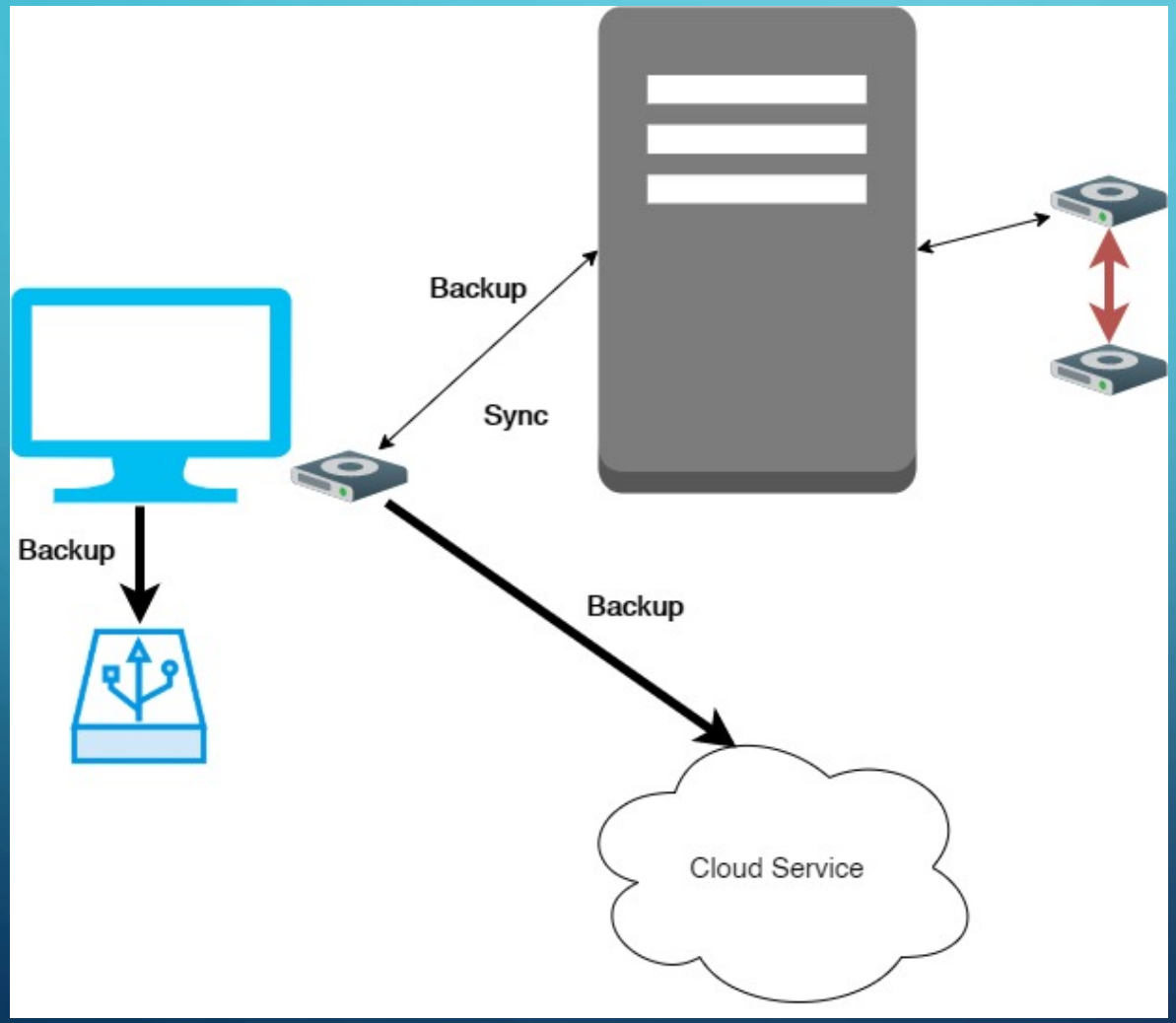
- 客户不一定喜欢与已经离职的人员接触
- 客户对已经离职的人员拥有自己在该人员前公司的数据也会表示担忧。
- 清理离职人员的信息是必要的。
- 配备属于公司的设备是必要的。
- 保密义务
- 获得许可

比较正确地使用电子邮件

- “写对邮箱地址”不像看上去那么简单
- 以加密方式发送敏感文件
- 不在邮件中包括敏感信息（比如密码）
- 看看cc的人是否都有权获取敏感信息
- 学会用bcc
- 不要轻易放一个文件的分享链接
- 当然还有更多的etiquette…



数据要多备份



因为你不想将你的电脑带出去请人恢复数据！

Filter by country:

Filter by violation (Art.):

All 5 5 6 7
8 9 12 13 14
15 16 17 18 21
24 25 28 29 30
31 32 33 34 35
36 37 58 83

Download on the App Store

under non-data protection laws (e.g. competition laws / electronic communication laws) and under "old" pre-GDPR-laws.

New features: "ETid" and "Direct URL"!
We have assigned a unique and permanent ID to each fine in our database, which makes it possible to precisely address fines, e.g. in publications. Once an "ETid" has been assigned to a fine, it remains the same, even if the fine is overturned or amended by courts at a later date, or if we add fines that were issued chronologically before. The "Direct URL" (click "+" or on a specific ETid to view details of a fine) can be used to share fines online, e.g. on Twitter or other media.

Show 10 entries

Search:

	ETid	Country	Date	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
	Filter Colum	Filter Column		Filter Column	Filter Column		Filter Column	
+	ETid-535	FRANCE	2021-01-27	150,000	Unknown	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link
+	ETid-536	FRANCE	2021-01-27	75,000	Unknown	Art. 32 GDPR	Insufficient technical and organisational measures to ensure information security	link
+	ETid-533	BELGIUM	2021-01-22	25,000	Unknown	Art. 5 (1) f), (2) GDPR, Art. 24 GDPR, Art. 32 GDPR, Art. 33 (1), (5) GDPR, Art. 34 (1) GDPR	Insufficient technical and organisational measures to ensure information security	link
+	ETid-529	SPAIN	2021-01-21	50,000	Alterna Operador Integral S.L.	Art. 6 (1) b) GDPR	Insufficient legal basis for data processing	link
+	ETid-534	SPAIN	2021-01-21	75,000	Telefónica Móviles España, SAU	Art. 6 (1) GDPR	Insufficient legal basis for data processing	link
+	ETid-528	SPAIN	2021-01-20	1,200	Individual	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles	link
+	ETid-530	NORWAY	2021-01-19	9,700	Aquateknikk AS	Art. 5 GPDR, Art. 6 GDPR	Insufficient legal basis for data processing	link
+	ETid-525	NORWAY	2021-01-14	38,600	Coop Finnmark SA	Art. 5 (1) a) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing	link
+	ETid-522	SPAIN	2021-01-13	6,000,000	Caixabank S.A.	Art. 6 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient legal basis for data processing	link
+	ETid-524	NORWAY	2021-01-12	38,600	Unknown	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing	link

王先生诉腾讯案、抖音诉腾讯案

- 南山法院认为，王先生所主张的微信好友关系既未包含其不愿为他人所知晓的私密关系，他人也无法通过其微信好友关系对其人格作出判断从而导致其遭受负面或不当评价，故认定王先生所主张的微信好友关系也 不属于原告的隐私。据此 驳回王先生的诉讼请求。
- 争论的核心：腾讯认为用户的头像、昵称等用户数据都属于腾讯公司的“商业资源”，除非腾讯同意，其他任何产品，即使获得用户授权，也不能使用这些用户的相关数据，否则即构成腾讯所谓“非法使用”。

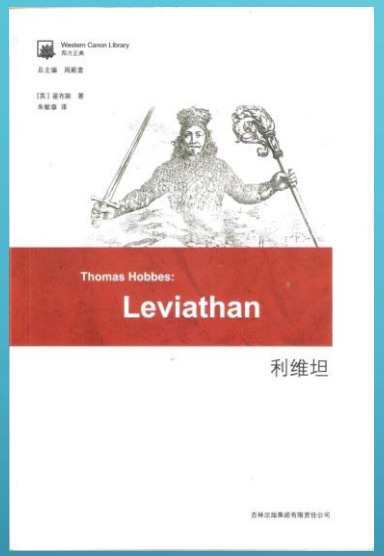
	申报数据	观察数据	推导数据
唯一为我拥有	唯一拥有权	联合拥有权	联合拥有权
多方共同拥有	联合拥有权	联合拥有权	联合拥有权
每人拥有（公共领域）	联合拥有权	联合拥有权	联合拥有权

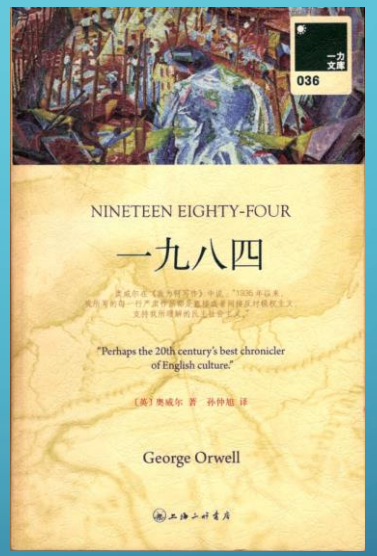
表格来自我的另一本译作《搜索：开启智能时代的新引擎》

隐私不等于安全

现实情况是，数据很安全，但隐私防护“漏得像个筛子一样”

扩展阅读





以及各相关法律条文

任老师随便聊

任氏有无轩：https://rsywx.net