

人工智能创新与伦理：青少年 在线隐私风险与保护

北京师范大学新闻传播学院

目录

- 引子：青少年隐私安全问题
- 一、青少年在线隐私风险和保护现状
- 二、人工智能创新带来的隐私风险
- 三、如何保护青少年的隐私

▼
引子：青少年隐私安全问题

一、青少年隐私安全问题

➤ 1.小红书被曝推送未成年人身体隐私

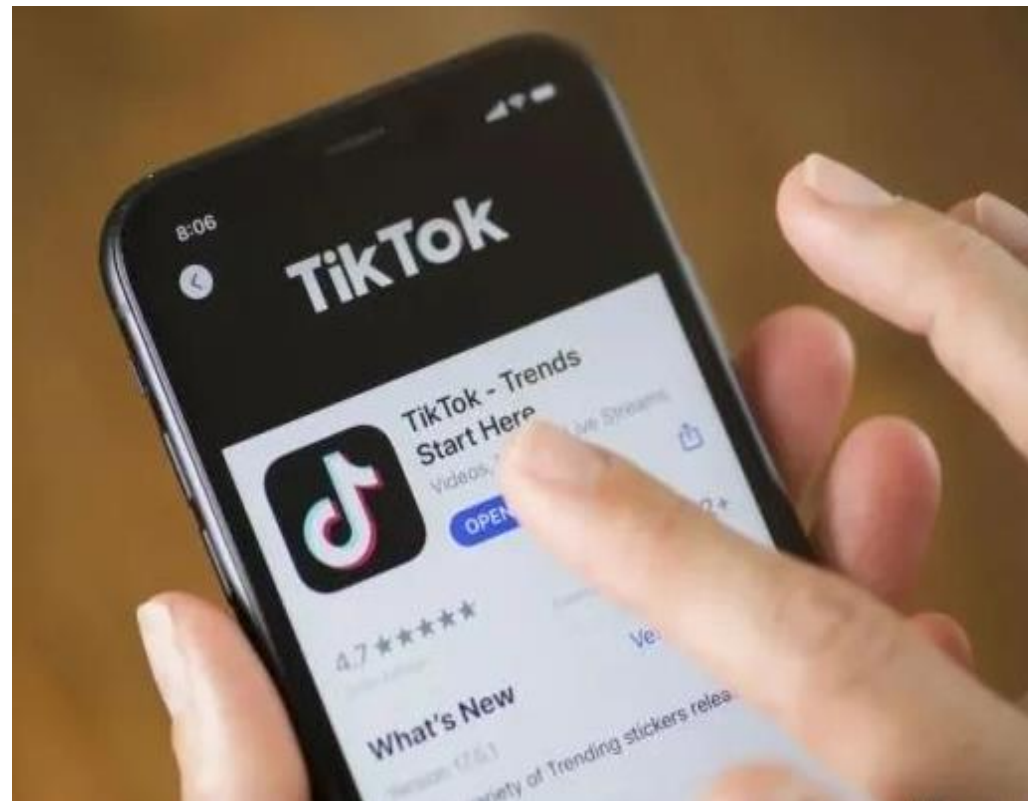
- 21年9月，四川成都的小学生家长蒋先生在“小红书”APP上搜索亲子乐园时发现，APP不时给自己推送含有大量未成年人生活的短视频，随后，越来越多明显泄露未成年人身体隐私的视频被推送过来.....
- 记者发现，视频拍摄者都是未成年人本人，拿手机自拍时镜头直接对准了自己的隐私部位。
- 在含有未成年人的短视频中，还有大量的用户留言、弹幕，有的留言带有强烈的性暗示。



一、青少年隐私安全问题

➤ 2.TIK TOK 非法收集青少年隐私信息

- 2020年4月，四名美国的青少年父母将TikTok和字节跳动告上法庭，称TikTok的一些滤镜和互动游戏需要通过面部扫描完成，但TikTok并未告知用户该信息收集行为，也未披露将如何使用这些数据，违反了当地保护个人生物识别信息的法律。
- 此次集体诉讼的原告中，青少年多达24人。最终TikTok同意支付9200万美元（折合人民币5.94亿元）。



一、青少年隐私安全问题

➤ 3.杭州未成年人隐私泄露

- 徐某（化名）偷录、存储同学陈某（化名）的隐私视频。事后，同学王某（化名）向徐某索要该视频，并通过社交软件转发致使视频在网络间传播，还曾在网上对陈某进行言语骚扰及威胁。视频扩散后，陈某遭受同学欺凌，心理受创，其法定代理人报案并向检察机关申援。
- 上城区检察院在工作中，委托专家对陈某进行心理评估和干预，疏导了陈某的负面情绪；联合公安机关调查取证，查清了网络传播隐私视频的侵权行为。因陈某希望通过法律途径保护自己的隐私及正常生活，保障陈某及时获得了专业的法律援助。



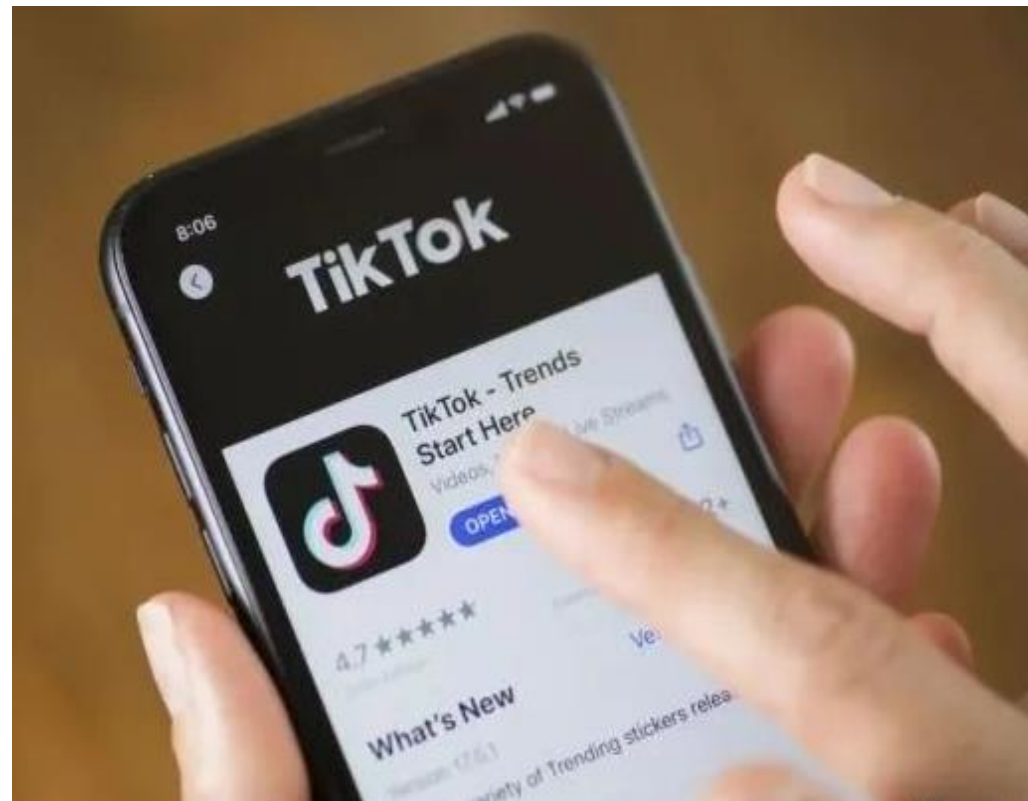


二、青少年在线隐私风险和保护现状

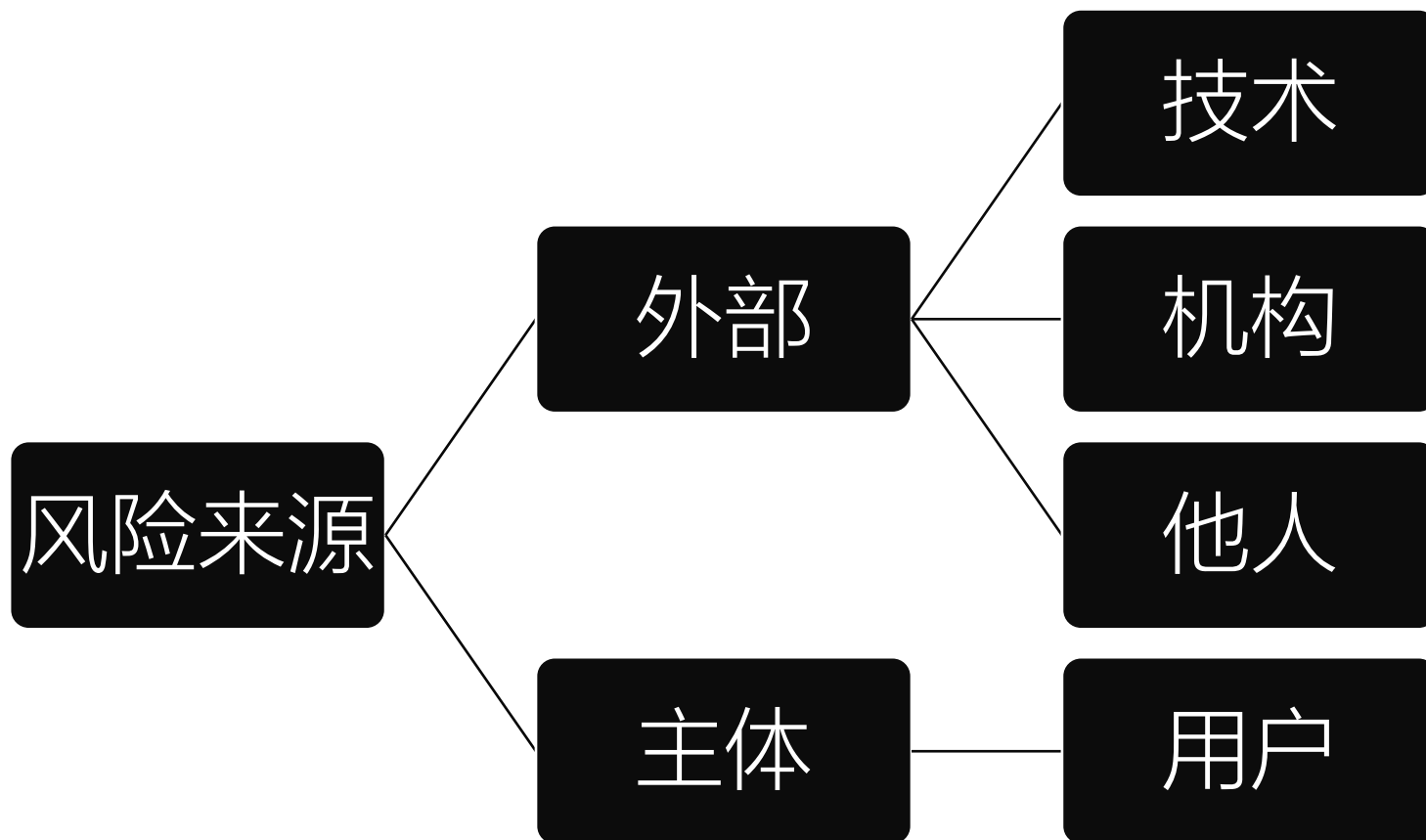
二、青少年在线隐私风险和保护

1. 网络安全的定义

- 网络安全是一个相对宽泛的概念，在宏观、中观与微观三个层面各有其指涉，包含网络信息安全、网络系统安全、网络文化安全、网络环境安全与网络使用安全等多个维度，具备保密性、完整性、可用性、可控性和不可抵赖性等安全的一般特点。



在线隐私风险来源



基于 117 个 APP 隐私风险的内容分析-集中性问题

序号	集中性问题	对应 App 数量/个	占总样本 App 比重/%
1	第三方可用平台用户信息/收集信息共享	50	42.7
2	用第三方账号登陆可以获取第三方的相关账号信息	40	34.2
3	默认授权平台可获第三方信息或进行相关操作	35	28.2
4	使用第三方服务但不负责/不适用	30	25.6
5	诱导接入第三方,且间接获取信息	29	24.4
6	广告投放、分析偏好,精准画像	27	22.2
7	平台对第三方的管理缺位	15	12.3
8	其他存在如无法完全删除痕迹、合并收购资产转让使第三方分享信息、因通讯好友使用而被读取信息、过度收集信息、第三方氛围表述模糊等问题	少于 12	<10

基于 117 个 APP 隐私风险的内容分析-各类 App 的主要风险问题

应用类型	主要问题	应用类型	主要问题
1. 地图导航类	收集第三方平台中的用户信息	21. 演出票务类	平台与第三方共享信息
2. 网络约车类	收集第三方平台中的用户信息	22. 实用工具类	第三方通过平台统计用户信息,且平台不对第三方信息保护措施负责
3. 即时通信类	无相对聚焦问题	23. 拍摄美化类	平台与第三方共享信息
4. 网络社区类	平台与第三方共享信息	24. 电子图书类	当通过平台链接至第三方,则默认个人信息向第三方平台分享
5. 网络支付类	平台不对第三方的隐私保护措施负责	25. 安全管理类	平台与第三方共享信息
6. 网上购物类	平台与第三方共享信息	26. 输入法类	同意平台的隐私政策即代表允许第三方平台收集用户信息
7. 餐饮外卖类	收集第三方平台中的用户信息	27. 浏览器类	平台不对第三方的隐私保护措施负责
8. 邮件快递类	收集第三方平台中的用户信息,精准用户画像	28. 运动健身类	平台与第三方共享用户信息
9. 交通票务类	无相对聚焦问题	29. 新闻资讯类	平台与第三方共享信息
10. 婚恋相亲类	平台通过第三方收集用户个人敏感信息,精准用户画像	30. 短视频类	平台利用隐私条款将商业行为合理化(未征得用户明确同意向用户投放广告);强制收集用户敏感信息
11. 网络招聘类	将用户简历、身份证号提供给第三方认证平台	31. 在线影音类	用户通过第三方账号登陆则默认授权平台读取第三方账号中的个人信息;平台读取用户敏感信息
12. 网络借贷类	平台与第三方共享信息且不对第三方的隐私保护措施负责	32. 网络直播类	用户在平台的浏览内容、个人信息等可能被平台合作方通过技术获取;平台读取用户信息并与第三方共享以分析广告偏好
13. 房屋租赁类	留存用户个人敏感信息,精准用户画像	33. 远程会议类	平台读取用户信息并与第三方共享以分析广告偏好
14. 二手车交易	无相对聚焦问题	34. 邮箱网盘类	平台读取用户信息并与第三方共享以分析广告偏好
15. 问诊挂号类	平台与第三方共享信息	35. 手机银行类	平台读取用户敏感信息并收集第三方账户信息
16. 旅游服务类	平台与第三方共享信息,精准用户画像	36. 投资理财类	平台收集第三方账户信息
17. 酒店服务类	收集第三方平台中的用户信息	37. 用车服务类	用户登陆平台即默认授权第三方相关操作
18. 网络游戏类	平台与第三方共享信息,存在隐私泄露风险	38. 女性健康类	平台与第三方共享信息并分析用户偏好以进行广告投放;平台检索用户的手机后台数据
19. 学习教育类	收集第三方平台中的用户信息	39. 本地生活类	收集第三方平台中的用户信息以分析用户偏好;默认读取用户地理位置
20. 应用商店类	通过平台服务外接第三方且与第三方共享信息		

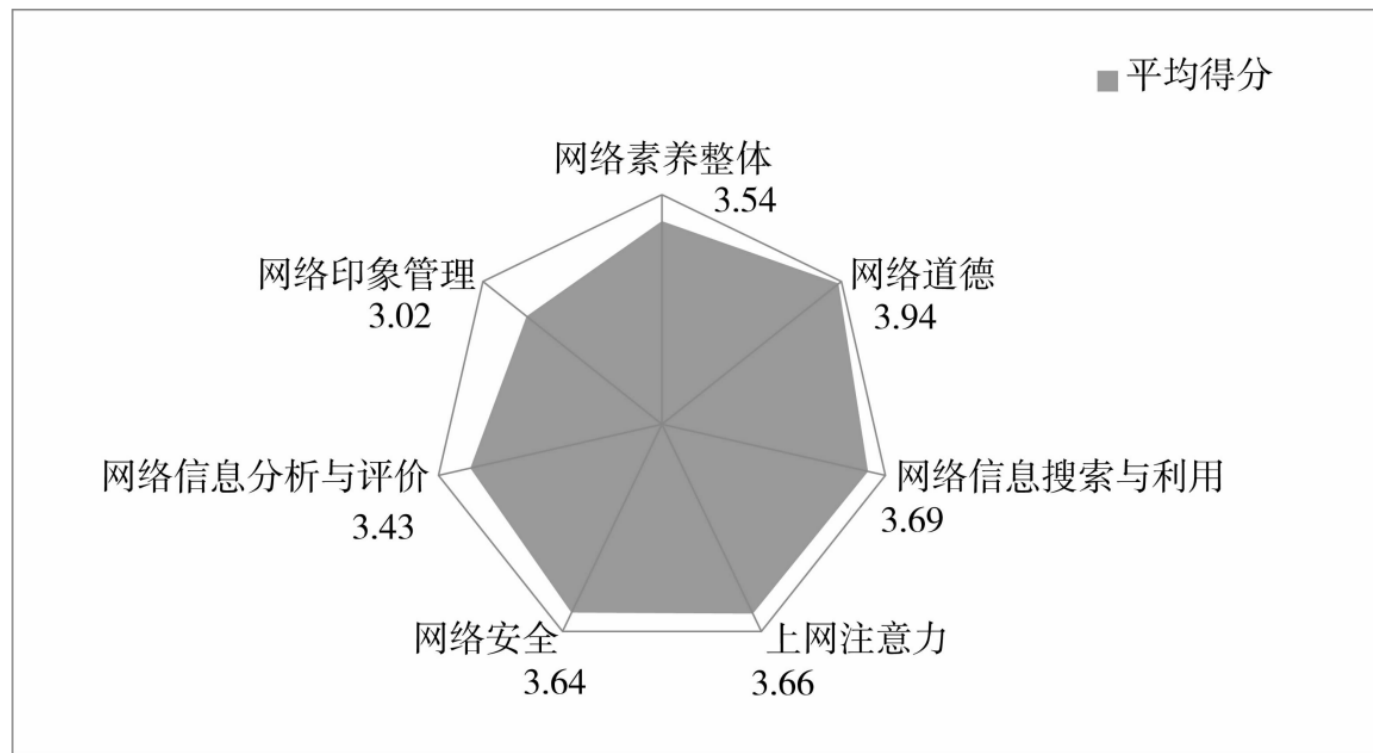
二、青少年在线隐私风险和保护

- 课题组将青少年的网络安全认知和行为作为媒介素养测量的一个重要维度，定义上更近似于个人层面的定义，重点关注个人对网络与信息风险的认知、判断及相关行为。
 - 我了解网络信息安全的作用（网络安全认知）
 - 我了解网络信息安全相关的法律法规和政策（网络安全认知）
 - 我总是下载官方正版软件（网络安全认知）
 - 我总是设置安全级别较高的密码（自我隐私和安全保护）
 - 我会在不同的网络应用上设置不同的密码（自我隐私和安全保护）
 - 我会使用杀毒软件杀毒（自我隐私和安全保护）
 - 我能够定时备份重要资料（自我隐私和安全保护）
 - 出现网络信息安全问题时，我能找到办法解决（自我隐私和安全保护）
 - 上网时，我在非必要情况下也填写过自己的真实信息（自我隐私和安全保护）
 - 我会对自己的上网设备进行隐私设置（自我隐私和安全保护）

二、青少年在线隐私风险和保护

3. 青少年网络素养现状

- 调查显示，青少年网络素养平均得分为3.54分（满分5分），略高于及格线，有待进一步提升。
- 其中，网络安全的平均得分最为3.64。



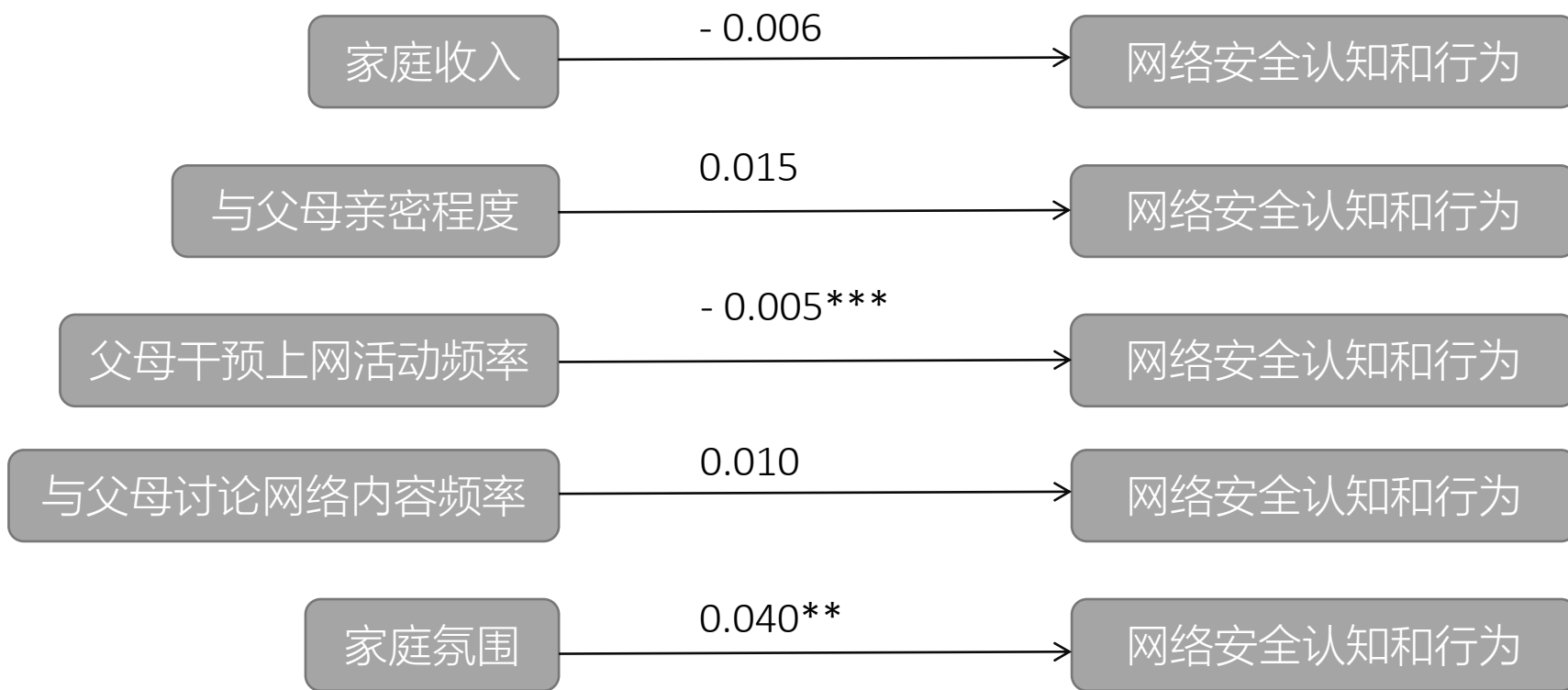
二、青少年在线隐私风险和保护

4. 个人属性对网络安全认知的影响分析



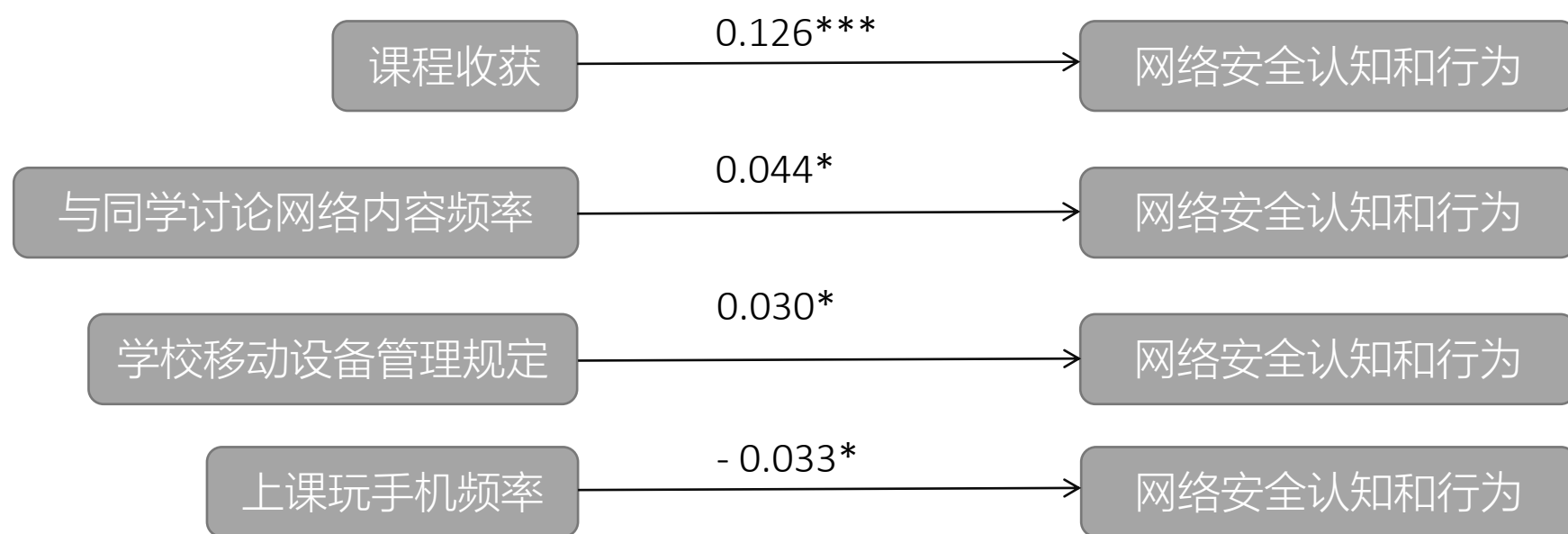
二、青少年在线隐私风险和保护

5. 家庭属性对网络安全认知的影响分析



二、青少年在线隐私风险和保护

6. 学校属性对网络安全认知的影响分析





二、人工智能创新带来的隐私风险

三、人工智能带来的隐私风险

➤ 1.人工智能增强了对隐私的直接监控能力

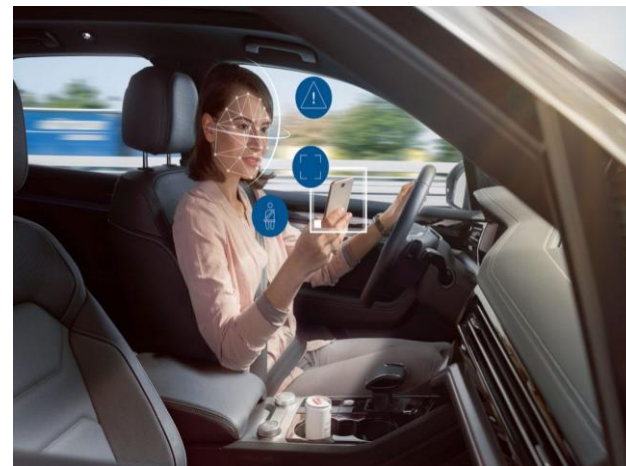
- 近年来，各式各样带有传感器和处理器的人工智能产品不断涌入人们的学习、工作和生活中，极大地增强了对隐私的直接监控能力。
- **例如：**语音识别技术的智能助手正在记录着你们所说的每一个字；而借助图像识别技术，无处不在的数字摄像头可以精准地从人群中自动识别人脸，锁定监控对象，甚至预测和判断人的行为。
- 央视 2021 年的“3·15”晚会上，记者曾报道某汽车销售商店为增加销售收入，专门安装了智能人脸识别探头，该探头对应的设备甚至可以直接判断进入店铺顾客的情绪是否“平静”。



三、人工智能带来的隐私风险

➤ 2.人工智能带来了更多的隐私获取性

- 这表现在各种新型人工智能产品层出不穷，使得原本私密的空间和信息不断受到侵蚀。
- **例如：**自动驾驶技术使得汽车这一原本较为私密的空间成为了数据收集空间，人们在车内的一举一动都将被记录在线，以往私密的出行信息也将被全面获取。
- 同样，在可预见的未来，机器人医生、机器人伴侣、机器人宠物等人工智能产品将走进千家万户，成为我们家庭生活的重要组成部分，在提供极大便利的同时，也将给获取隐私带来了更多新的获取点。



三、人工智能带来的隐私风险

➤ 3.人工智能具有超强的“画像识别”能力

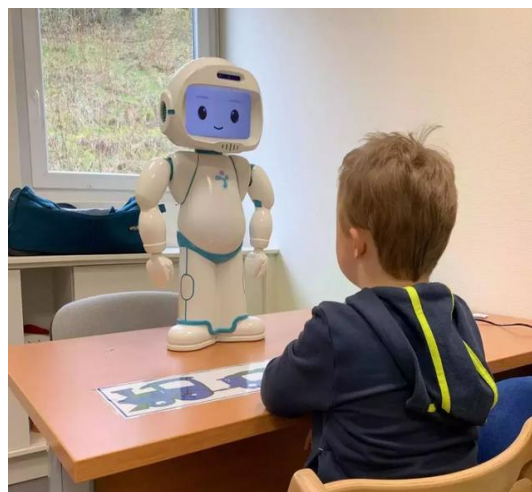
- 借助物联网、大数据等技术，人工智能的数据整合和分析能力得到极大的增强，能够轻易地描绘出用户的完整“画像”，也就是通过对智能技术挖掘到的用户数据进行深度整合，分析其个人喜好、行为习惯、消费能力等，从而制订个性化服务方案。
- **例如：**一个习惯于购买两百元左右价位服装的用户，收到两千元价位服装“精准广告”的概率极低；一个喜欢时尚服装品牌的用户，也不太可能收到民族风的服装广告。
- 最终每个用户在智能技术面前都已经成为“透明人”。在不经意间，他们已经被日常的网络行为形塑成某种类型的用户，并被不断强化。



三、人工智能带来的隐私风险

➤ 4.人工智能本身将成为隐私信息的载体

- 人工智能的社交性质可能会产生一种新的高度敏感的隐私信息，被称之为“设置隐私”（setting privacy）。具言之，在可预见的未来社会，社交型机器人将会在人们的生活中扮演重要角色，为人们提供陪伴、聊天、学习、看护等服务。随着与可编程的社交型机器人交互的不断深入，人们将逐渐展现其最为私密的心理属性(psychological attributes)。
- 此时，这些人工智能的设置信息将变得无比重要，因为它们负载着人们的隐私，透露着人们在机器人身上设置了哪些“陪伴程序”。对此，读取人们是如何编程以及与机器人交互的设置信息，就像读取人们与一个心理学家的谈话一样，相关的隐私将一览无遗。



三、人工智能带来的隐私风险

➤ 5.人工智能侵害隐私的行为具有迷惑性。

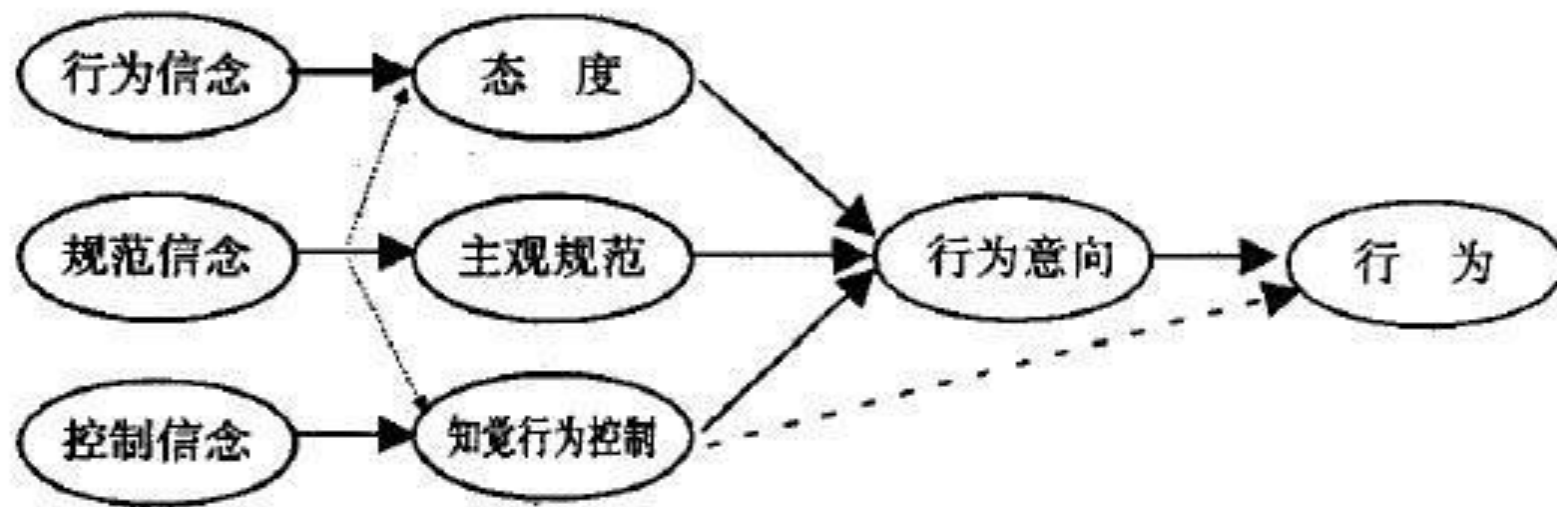
- 相较于其他形式的隐私入侵科技，由于人工智能的外形、声音、思维等与人类相仿，因而人们更加愿意接受它们。
- **例如：**具备人形外表的社交型机器人常常被用于照顾老人和残疾人，或者被用来解决自闭症等儿童问题。然而，随着人工智能越来越像人类，人们也会越来越将它们视为准人类或克隆人，而非单纯的工具，这使得它们的隐私入侵行为更具迷惑性。逐渐地，人们更加愿意与聊天机器人互诉衷肠，向机器人医生袒露病情，因为它们看上去是那么的值得信任，以至于人们根本不会察觉它们潜在的隐私风险。
- 对此，福格教授曾经深入分析过这种极具迷惑性科技的危险，一方面，它们具有善良可爱的外表和忠诚可靠的良好口碑，这使得它们极易获得人们的信任，隐藏潜在的危险意图；另一方面，它们又极具智慧属性，能够预测人们的情绪和行为，迎合人们的心理需求。





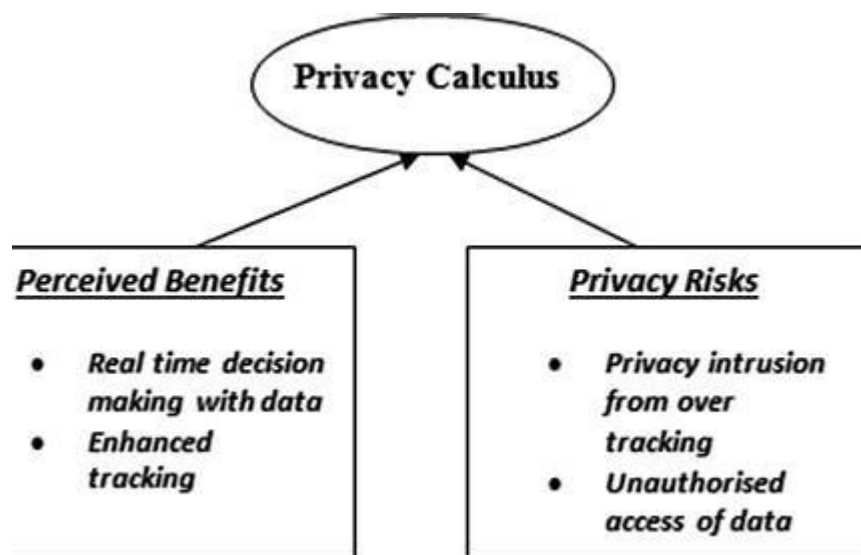
三、如何保护青少年的隐私

三种理解个人在线隐私的研究视角- 计划行为视角



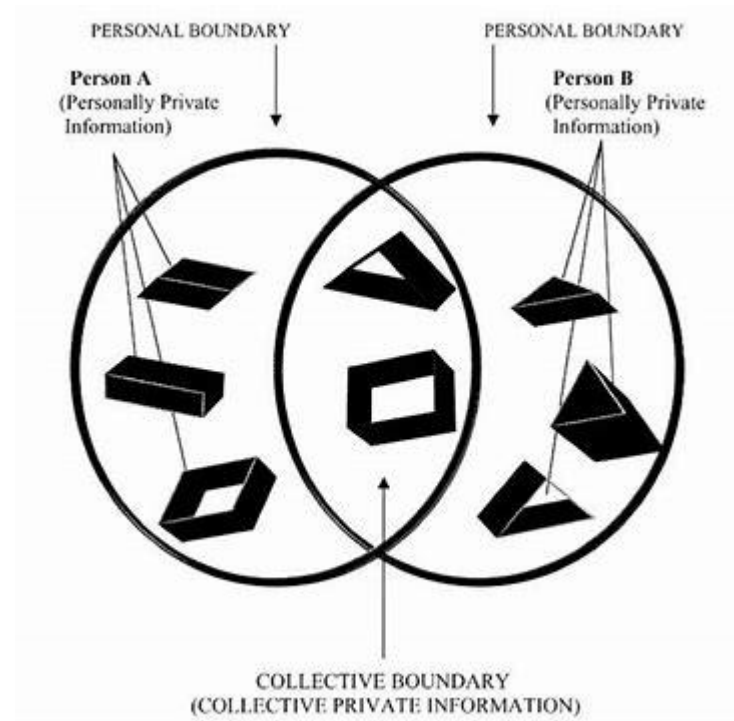
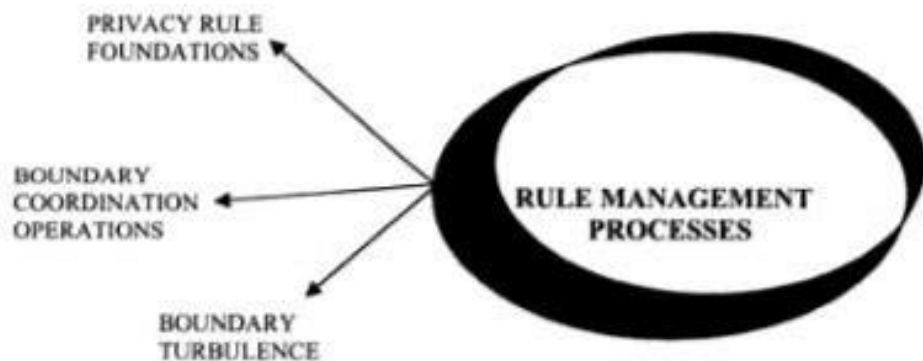
启示：加强教育，提高隐私风险保护意识和知识；呼吁社会共识

三种理解个人在线隐私的研究视角- 风险-收益视角



启示：不可控，使用就有风险！加强法律法规建设

三种理解个人在线隐私的研究视角- 边界管理视角



启示：隐私保护是动态的，需要我们持续关注，共同合作！

四、如何保护青少年的隐私

➤ 1.完善青少年隐私保护的法律法规

- 目前，我国已经出台一系列涉及学生隐私保护的法律法规，其中既包括总揽网络信息安全的《网络安全法》，也包括涉及隐私保护主体的《未成年人保护法》和《未成年人网络保护条例（送审稿）》，还包括针对应用服务提供者做出要求的《移动互联网应用程序信息服务管理规定》。
- 法律法规虽然不少，**但问题在于相关条款内容都是原则性要求，可操作性不强。**应该尽快出台实施细则，明确界定学生线上行为范围、被采集信息的使用目的和方式，规范用户协议中的具体隐私条款内容，开展隐私保护专业技术测评。在完善同意机制中，**对于涉及青少年个人信息处理的情形，应当特别取得其监护人的同意。**



四、如何保护青少年的隐私

➤ 2.学校加强隐私风险科普和法制宣传教育

- 学校要加大青少年网络知识的宣传与普及，**让青少年明白网络隐私侵权行为的隐匿性、迷惑性、危险性**。定期定时定点聘请专业法律人士开展主题讲座，开通青少年法律网站，出版青少年网上法律手册，加强其上网的警惕和安全意识，从而强化青少年自我保护能力。
- 此外，营造积极、良好的网络行为氛围，号召实施《青少年网络文明公约》，争做文明上网好公民。学校还可以成立青少年隐私权保护的专门机构，主要负责青少年投诉和维权工作，切实保护好青少年的合法权益。



四、如何保护青少年的隐私

➤ 3.家庭教育强化隐私保护意识和上网行为监督

- 家庭教育所提供的亲情场所是学校教育所不能及的，青少年相关家庭成员对网络隐私风险和保护意识的高低会对孩子产生直接的影响。
- 有研究表明，青少年社交网络隐私保护行为主要受到父母的主观规范影响。随着父母教育程度的提高，对网络知识尤其网络隐私问题的关注与了解也会随之增加。
- 出于对隐私泄露问题的担忧，接受过本科教育甚至研究生教育的父母比本科以下教育程度的父母更倾向于干涉子女上网自由。这种干涉事实上能够促使青少年采取更多隐私保护行为。



四、如何保护青少年的隐私

➤ 3.家庭教育强化隐私保护意识和上网行为监督

- 因此，在家庭教育中，青少年的父母或者其他监护人应当提高自身的隐私保护和安全意识，规范自身使用网路的行为，并学习一定的教育方法，加强对青少年使用网路行为的正确指引和监督，经常与青少年分享使用网路时应该注意的隐私问题，在生活的点点滴滴中，强化隐私保护安全意识。
- **例如：**北京师范大学教育新闻与传媒研究中心编译推出了《数字时代背景下家长行动指南》，在“保护隐私”章节中，授以家长具体的操作措施，包括如何帮助孩子创建一个安全的密码、如何帮助孩子使用社交网络的隐私设置功能等。





**THANK
YOU**