arXiv:2305.05004v2 [cs.CR] 8 Oct 2023

可用隐私与安全研究有多 WEIRD？（扩展版）

Ayako A. Hasegawa DaisukeInoue Mitsuaki Akiyama*NICT*
NICTNTT

摘要

在人机交互（HCI）和心理学等人因领域，研究人员一直担心参与者大多来自 WEIRD（西方、受教育程度高、工业化、富裕和民主）国家。这种 WEIRD 偏倚可能会妨碍我们了解不同人群及其文化差异。可用隐私与安全（UPS）领域沿用了许多人因领域研究中的研究方法。我们开展了文献综述，以了解 UPS论文中的参与者样本在多大程度上来自 WEIRD国家，以及招募西方或非西方参与者的各项用户研究所采用的研究方法和研究主题的特点。我们发现，UPS领域对 WEIRD国家的偏倚程度高于人机交互领域。研究方法和招募方法中的地理与语言障碍，可能会导致研究人员在本地开展用户研究。此外，许多论文未报告参与者人口统计信息，这可能妨碍对所报告研究的复现，导致可复现性较低。为提高地理多样性，我们提出以下建议：促进复现研究，解决研究/招募方法中的地理与语言问题，并推动针对非 WEIRD人群相关主题的研究。

1 引言

可用隐私与安全（UPS）研究关注技术使用者（即人类）的视角，而传统安全研究尚未涉及这一视角。它有助于解决社会需求与技术可行性之间的鸿沟所引发的安全与隐私问题，即社会技术鸿沟 [5]。UPS领域已有约四分之一个世纪的研究历史。UPS论文已发表于安全与隐私领域内外的多个会议和期刊上，UPS论文的发表数量也逐年增加。1996年，Zurko和Simon在论文中提出了UPS这一概念，并将其称为以用户为中心的安全。随后，两篇开创性的UPS论文于1999年发表。Adams和Sasse主张在设计安全机制时应考虑人因 [7]。此外，Whitten和Tygar指出，安全领域缺乏良好的用户界面设计，并通过签名和加密电子邮件，采用了多种可用性测试方法 [109]。

UPS的研究方法，即招募参与者并开展用户研究，通常具有跨学科性质。许多此类研究方法源自人机交互（HCI）、心理学和行为科学。在这些研究领域，据报告，大多数参与者来自西方，这带来了一个问题：多年来积累的许多研究发现可能无法推广到其他国家和文化。Henrich等人指出，美国参与者在许多心理测量指标上都是常见的离群值，这一事实使这些参与者被称为“WEIRD”（西方、受教育、工业化、富裕和民主） [43]。Linxen等人 [61] 于2021年发表了一篇题为“CHI有多WEIRD？”的论文，他们在文献综述中通过定量分析证实了人机交互领域顶级会议之一CHI的参与者样本存在WEIRD偏倚。由于WEIRD国家的居民仅占世界人口的少数，因此有人认为这一事实会显著影响人机交互研究的可推广性。尽管WEIRD框架依据国家统计数据或特征设定指标来评估参与者抽样，但存在局限性（例如，在全球南方，个别富裕人士可能更容易接触到），它仍成功地概括了参与者的地理多样性。

在 UPS 研究中，一些研究还发现，WEIRD 与非 WEIRD 社会／人群之间在安全与隐私方面存在关键差异，这些差异源于环境因素（例如 IT资源使用、文档以及

本文是发表于 USENIX SECURITY 2024 的论文的扩展版本。

法律/法规）和个人因素（例如认知（或误解）、偏好和易受影响程度） [8, 11, 20, 44, 54, 58, 59, 87]。我们进一步假设，人口统计偏差也可能影响攻击可行性。UPS 研究人员有时会借助用户研究来证明攻击的可行性，这是 UPS 研究的一种独特方法。这些观察结果表明，基于传统 WEIRD偏倚研究发现提出的威胁评估、设计启示、干预措施和支持技术，可能无法充分惠及多元化的非 WEIRD 社会／人群，也未必能在其中付诸实践，反而可能阻碍这些社会／人群安全与隐私水平的提升。尽管 WEIRD 偏倚会对 UPS 研究造成危害，但 UPS 研究在地域广度方面的程度以及阻碍地域多样性的因素，尚未得到充分调查。此外，从 WEIRD 视角来看，所采用的研究方法和所探讨的主题仍未被揭示或遭到忽视。本研究对 UPS 领域开展系统性文献综述，以回答以下研究问题（RQs）。

RQ1：*UPS*论文中的参与者样本在多大程度上来自*WEIRD*国家？这种情况随时间发生了怎样的变化？
RQ2：招募西方参与者或非西方参与者的各项用户研究，在研究方法和研究主题的特征上有哪些差异？

我们回顾了近期五年（2017–2021年）内安全与人机交互领域具有代表性的会议上发表的715篇招募了参与者的UPS论文。我们依据提取的参与者信息，使用WEIRD框架评估参与者样本的地理多样性，并分析了作者所属机构、研究方法和研究主题。我们发现，UPS论文中的绝大多数参与者样本都偏向WEIRD国家，尤其是西方参与者样本（78.89%）。这一偏差高于Linxen等人对CHI论文进行回顾所得的结果（73.13%）。Linxen等人报告称，过去五年中，CHI论文里的非西方参与者样本比例大幅上升（从16.31%增至30.24%，为原来的1.85倍）；而我们的结果显示，UPS论文中的这一比例有所下降（从25.00%降至20.77%，为原来的0.93倍）。作者往往会从其所属机构所在国家招募方便获取的参与者，例如，当地大学的学生，他们很容易被大学研究人员接触到。由于大多数作者隶属西方国家的机构，参与者样本更有可能偏向西方人。此外，我们发现，不少论文未报告参与者人口统计信息。这种情况在非人机交互会议和非以用户隐私与安全为重点的会议中尤为明显。此类可复现性较低的论文可能会妨碍复现研究。我们确认，每个研究主题都存在明显的西方偏差。尤其是攻击可行性研究严重偏向西方，且存在人口统计方面的问题：攻击的可行性可能会受到以下因素的影响：参与者人口统计信息，因为这类研究依赖目标对象的英语水平。

我们提出以下建议，以使UPS研究减少WEIRD倾向。首先，应促进UPS领域的复现研究，因为大多数UPS论文只考察了WEIRD国家，并未考虑或讨论地理多样性是否会影响研究结果。其次，应处理研究地点和招募方法方面的地理问题。第三，研究人员也应更加多元化（例如，纳入非西方研究人员），以克服语言障碍，与非WEIRD人群进行准确、深入的交流并理解他们。最后，我们讨论了未来需要关注的UPS研究主题。

2 背景与相关工作

2.1 原始研究：CHI 有多 WEIRD?

Linxen等人在2021年发表了一篇题为“CHI有多WEIRD？”的论文（以下简称Linxen研究） [61]。Linxen研究的动机源于心理学中提出的问题：(1)心理学中的大多数研究发现都基于美国本科生 [14]；(2)与来自其他国家的研究发现相比，来自美国参与者的研究发现往往是离群值 [43]。随后，Linxen等人调查了2016–2020年间在CHI这一人机交互领域最负盛名的学术会议上发表的2,768篇论文中招募的参与者的地理多样性。他们表明，CHI论文的参与者样本高度偏向WEIRD国家，例如，73.13%的参与者样本来自西方国家。然而，令人鼓舞的是，他们还表明，近年来非西方参与者样本的比例一直在增加。

2.2 WEIRD 偏倚对 UPS研究的危害

一些 UPS研究聚焦于非 WEIRD 社会/人群，并发现 WEIRD 与非 WEIRD 社会/人群在安全和隐私方面存在关键差异，这些差异源于环境和个人因素。这些结果揭示了对 UPS研究造成的现实及潜在危害：基于传统 WEIRD偏倚研究的发现而提出的设计启示、干预措施和支持技术，可能无法充分惠及非 WEIRD 社会/人群，也未必能在其中切实应用。

环境因素。据报道，WEIRD与非 WEIRD 社会／人群在环境因素方面存在差异，例如 IT资源使用、文档以及法律/法规。首先是 IT资源使用方面的差异。在 WEIRD 社会中，人们通常各自拥有设备；而在非 WEIRD 社会中，经济条件限制、社会价值观和社会权力关系等文化情境促使人们共享

设备，这种做法带来了保障个人隐私的新挑战 [8]。特别是，若干研究报告指出，在性别不平等程度高于西方国家的全球南方，女性使用 IT资源时更容易遭受隐私侵害、骚扰和欺诈 [11, 87]。其次是文档方面的差异。安全与隐私文档（例如建议、指南和培训材料）会显著影响个人的安全与隐私实践 [84, 112]。例如，美国发布了许多重要的安全与隐私文档，如 NIST SP-800 系列 [72], , 其他国家也会引用这些文档。然而，由于英语水平较低且翻译需要额外成本，这些文档在非英语国家的普及程度远不及英语国家 [42, 54]。第三是法律/法规方面的差异。数据隐私法和法规在保护个人隐私权、推动服务提供商负责任地开展数据实践方面发挥着至关重要的作用。许多研究考察了服务是否遵守法律和法规（例如欧盟《通用数据保护条例》），以及符合法律要求的界面对用户隐私的可用性 [73, 102]。然而，除欧洲和美国外，亚洲、南美洲和非洲等地区的许多国家也已独立制定了大量数据隐私法 [26, 49],，这表明不同国家的服务在用户隐私处理方式上可能存在差异。此外，尚未制定数据隐私法的国家通常被上述基于现有隐私法和法规的研究方法所忽视。

个人层面因素。研究还指出，个人层面因素也存在差距，例如（错误）认知、偏好和易受攻击性。需要注意的是，个人与其周围环境并非相互独立的实体，因为个人会受到环境的影响 [57, 95]。首先是（错误）认知方面的差距。许多研究发现，对安全与隐私技术的错误认知会导致不安全行为，并增加用户受到伤害的风险 [4, 94]。然而，Herbert 等人发现，影响用户错误认知的最重要因素之一是居住国，西方国家与非西方国家之间的差异尤为显著 [44]。这一结果表明，有必要进一步探究这些差异的成因，以及如何针对各个国家纠正错误认知。其次是偏好方面的差距。许多研究探讨了用户在是否愿意与公司共享数据、是否愿意在社交媒体上披露数据方面的隐私偏好，并提出了基于用户隐私偏好推荐隐私设置的技术 [55, 96, 108]。一些研究报告称，这类隐私偏好因国家而异 [22, 58, 59]。例如，Li 等人表明，当用户得知第三方公司须对数据收集行为负责时，来自集体主义国家（如中国）的用户分享数据的意愿较低，而来自个人主义国家（如美国）的用户分享数据的意愿较高 [59]。第三是易受攻击性方面的差距。许多研究识别了攻击者的网络钓鱼手法和用户的应对策略，并提出了干预措施 [35, 103, 106]。然而，Butavicius 等人发现，来自个人主义文化的用户受网络钓鱼邮件影响的可能性显著较低 [20],，这表明集体主义国家的用户可能更容易暴露于网络钓鱼威胁之下。此外，Hasegawa 等人揭示，非英语母语者针对英语可疑邮件和母语可疑邮件采用了不同的应对策略 [42]。

受这些观察结果的启发，我们聚焦于 UPS 中的 WEIRD视角。确保安全与隐私并不局限于 WEIRD社会，而是一项共同的全球性挑战。为了努力在全球范围内公平地提供安全与隐私，UPS必须扩大关注范围，纳入非 WEIRD社会；具体而言，了解 WEIRD社会/人口群体与非 WEIRD社会/人口群体之间的相似之处和差异，对于应对这一挑战至关重要。

2.3 UPS研究中的文献综述

许多研究人员围绕 UPS论文的“研究主题”开展了文献综述。Garfinkel 和 Lipford [37] 总结了整个 UPS领域的研究主题。其他综述则聚焦于 UPS特定子领域的研究主题，例如与隐私和安全相关的决策 [6],社会网络安全 [110],网络钓鱼干预 [35], 高风险用户 [105],性虐待 [74], 社交媒体中的跨文化隐私问题 [101],以及以开发者为中心的安全 [97]。

另一方面，很少有研究人员从 UPS论文的“方法论”角度开展文献综述。Distler等人开展了一项文献综述，以了解研究人员使用哪些方法，以及如何呈现参与者面临的风险 [32]。Kaur 等人回顾并比较了针对专家和非专家（终端用户）的 UPS论文所采用的方法 [53]。除了揭示当前的研究实践外，这些作者还指出了 UPS论文中的方法论和伦理挑战，例如没有对伦理上可接受的欺骗作出定义、未能运用理论解读结果，以及参与者多样性不足。

表 1 比较了我们的研究与密切相关的文献综述。我们的研究是 准复现Linxen研究 [61], , 该研究聚焦于人机交互领域用户研究参与者的WEIRD视角；我们聚焦于UPS领域。我们的研究在以下方面不同于两篇密切相关的UPS研究方法 [32, 53] 论文[1]:

[1]请注意，此比较基于简化后的要点，并未涵盖论文的所有目标。

表 1：我们的研究与以往关于用户研究的综述文献的比较。

论文	领域	人群	地理多样性	研究主题	会议	时期	# 论文*
Linxen等人 [61]	HCI	Any	从WEIRD视角进行分析	未分析	CHI	2016–2020	2,768
Distler等人 [32]	UPS	Any	未分析	已分析	S&P，SEC，CCS，SOUPS，CHI	2014年–2018	284
Kaur 等人 [53]	UPS	专家	从 W视角进行分析	分析	安全领域一级/二级 [40], SOUPS、CHI	2008–2018	48 (+48)**
我们的研究	UPS	Any	从 WEIRD 视角分析	已分析	S&P, SEC, CCS, NDSS, PETS, CHI, CSCW, SOUPS , USEC, EuroUSEC	2017–2021	715

*完整评审论文的数量。**他们审阅了48篇关于专家的论文，以及48篇关于非专家的论文，以进行比较。

- 我们从更多元化的会议中收集论文，以全面了解 UPS 论文。
- 我们评审了较新的论文（2017–2021）。
- 我们不仅分析参与者所在国家的西方程度，还分析这些国家在教育程度、工业化程度、富裕程度和民主程度方面的程度。
- 我们揭示了研究主题、会议和作者所属机构中的西方偏向程度。
- 我们讨论参与者的人口统计特征可能对 UPS 研究结果产生的影响，并推荐未来的 UPS 研究主题。

请注意，近期 Mathew等人报告了安全与隐私论文作者多样性的阶段性研究结果，其中部分涉及 UPS [64]。我们的研究不仅关注作者多样性，也关注参与者多样性。

3 方法论

3.1 评审流程

我们遵循了 UPS领域近期代表性综述论文所采用的评审流程 [32, 74]。

标准。 由于我们关注 UPS论文中招募的参与者在地理分布上的多样性，因此决定评审符合以下三项标准的论文：篇幅完整的论文，且 (i) 将人因以及计算机安全/隐私问题作为主要研究目标；(ii) 招募了自愿参与者；(iii) 报告了参与者总人数。我们剔除了以下不符合标准 (ii) 的论文：

- 分析在线公共数据的论文，例如在线服务设计和社交媒体帖子。
- 分析员工行为日志（例如，对模拟网络钓鱼的响应）或实际服务用户行为日志（例如，对浏览器上显示的警告的响应）的论文。
- 作者进行了民族志观察的论文。

第一阶段：会议筛选。我们决定回顾两篇近期具有代表性的论文中至少一篇所选取的所有会议，这两篇论文全面回顾了 UPS 论文 [32, 105]：S&P、USENIX Security (SEC)、CCS，NDSS 和 PETS（安全与隐私领域的顶级及第二梯队会议）、CHI 和 CSCW（人机交互领域的顶级会议），以及 SOUPS、EuroUSEC 和 USEC（专注于 UPS 的一个会议和若干研讨会）。2017–2021 年间，上述 10 个会议收录的全文论文总数为 7,587 篇，如表2所示。

第二阶段：筛选可能相关的论文。第一阶段的数据集包含大量非UPS安全论文（例如密码学理论）以及非UPS人机交互论文。为了排除不符合标准的论文，我们使用以下搜索查询对论文进行了筛选：*(security ORprivacy) AND(recruit* OR participant*ORrespondent*)*。由于我们特别关注招募了参与者的UPS论文，因此我们使用了术语招募、参与者和受访者，而没有使用适用于所有UPS论文的相关术语，例如用户或可用性。尽管先前的一项研究 [32] 对标题或摘要进行了类似的搜索，但我们对全文进行了搜索，以避免不恰当地过度排除论文。详细流程见附录A.1。我们的搜索查询共得到3,226篇可能相关的论文。

第三阶段：确定相关论文。第一作者审阅了这3,226篇论文的标题、摘要和正文，并剔除了不符合我们标准的论文。每当第一作者发现某篇论文是否符合标准尚不明确时，作者们便会讨论并解决这一问题。最后一位作者独立对随机选取的323篇论文（10%）进行了双重编码。评审者间信度的 Cohen's kappa系数为$k = .86$，这被认为是极佳的一致性水平 [34]。经过这次人工筛选，我们最终确定了715篇相关论文[2]。表3 列出了各出版年份中确定的 UPS论文数量。UPS论文的数量在2020–2021年显著增加，而 Distler等人和 Kaur 等人并未涵盖这一时期 [32, 53]。

第4阶段：详细审查。第一作者对每篇论文进行了详细审查，并提取了表4所列的出版物、参与者、作者及方法/主题相关信息。请注意，我们没有提取试点研究的信息。编码项目基于 Linxen研究 [61]，其中部分项目是本研究针对 UPS论文新增的。以下将介绍这些新增项目。

- **参与者类型** 是指参与者属于专家还是非专家（终端用户） [53]。
- **研究方法**和**招募方法**包括

[2]论文完整列表见附录 A.2。

表 2：评审流程各阶段中的 UPS论文数量。

论文	S&P	SEC	CCS	NDSS	PETS	CHI	CSCW	SOUPS	EuroUSEC	USEC	总计
# 5 年内发表的论文（第一阶段）	426	701	751	403	313	3,471	1,268	143	57	54	7,587
# 潜在相关论文（第二阶段）	139	191	233	108	137	1,379	797	137	54	51	3,226
# 相关论文（第三阶段）	45	81	48	28	53	177	63	125	48	47	715

表3：按发表年份统计的需进行详细审查的论文数量。

	2017	2018	2019	2020	2021	总计
# 论文	117	128	119	150	201	715

表4：每篇论文提取的信息。

类别	Item
出版	标题、会议、出版年份
参与者	人数*、居住国家*、教育*、收入*、 参与者类型（专家/非专家）*
作者	隶属机构、隶属机构所在国家
方法 和主题	研究方法*、招募方法*、研究主题， 设计评估（是/否）*、攻击可行性评估（是/否）*

星号表示这些信息是按每项用户研究而非每篇论文提取的。一篇论文可以开展多项用户研究。

表5：研究方法和主题。

Item	分类
研究 方法	调查、访谈、实验室研究、在线 现场实验，试验部署，其他
招募 方法	机构、众包、社交媒体、城市、 邮件列表/个人联系人、会议/活动、 网络样本库、源代码存储库、其他、未提及
研究 主题	总体而言，访问控制与隐私偏好， 身份验证、漏洞／恶意软件／事件响应 隐私侵害、社会工程、隐私增强 技术、其他

表中的分类 5。我们参考现有分类制定了这一分类 [32,53]。

- **研究主题**是表 5 中列出的分类（七个不同的主题和“其他”）。我们改进了现有的分类 [32]，重点关注技术（详情见附录 A.4）。

- **设计评估**是指作者是否对技术或服务设计进行了实验。例如，采用组间或组内方法比较多个界面或框架效应的论文，或明确说明已进行可用性评估的论文，均编码为“是”。

- **攻击可行性评估** 是 UPS 特有的：作者是否仅为了证明其提出的攻击的可行性而开展用户研究，并未询问参与者对安全与隐私问题的看法。

我们按每项用户研究而非每篇论文提取信息

如果一篇论文针对多项用户研究分别招募参与者，且这些研究采用不同的研究方法（例如调查和访谈）或有不同的目的（例如，一项调查用于识别用户关注点，另一项调查用于评估所提出的用户界面），如表 4。

一些论文对招募过程和参与者信息的描述含糊不清。此外，对每篇论文的研究主题进行分类可能存在困难。为减少编码人员的主观性，第一作者和最后一位作者多次讨论，以制定编码手册并解决他们在解读上的分歧。最后一位作者对随机选取的72篇论文（10%）进行了独立的双重编码。我们的综述的Cohen’s kappa系数为k = .85–.97，这被认为是一致性极佳的水平 [34]。

3.2 分析

我们遵循了 Linxen研究中采用的 WEIRD缩写分析框架 [61]。为了将 Linxen研究的结果（即人机交互领域）与我们的结果（即 UPS领域）直接比较，我们采用了与 Linxen 研究相同年份的国家统计数据 [3]。

参与者样本。 参与者样本的数量是指在用户研究中招募到参与者的国家数量。一篇论文可以报告多个参与者样本，也就是说，一篇论文可以从多个国家招募参与者。

WEIRD。 WEIRD缩写（西方、受教育、工业化、富裕和民主）是一组用于衡量参与者所在国家多样性的指标。一个国家并非西方国家，并不一定意味着它不是EIRD国家；也就是说，有些国家虽然非西方，却属于EIRD国家，例如以色列、日本和韩国。

- **西方**。 我们根据亨廷顿的分类，将每篇论文中提及的参与者所在国家划分为西方或非西方 [48]。该分类基于后冷战时代的文明划分，其中西方以欧洲和北美为中心。请注意，尽管我们在比较中采用了这一分类，但它在政治学界受到过批评 [24,36]，且并不总是符合人们对西方的一般认知。

  – 西方（示例）：美国、加拿大、英国、德国、荷兰、瑞士、瑞典和澳大利亚。

[3]The 统计数据由 Linxen研究的作者提供 。

– 非西方（示例）：印度、中国、日本、韩国、以色列、沙特阿拉伯、俄罗斯、巴基斯坦、孟加拉国、墨西哥、巴西和南非。

• **受过教育**。我们通过分析两个指标，全面探讨了参与者的教育水平：(a) 每个国家的平均受教育年限 [80] 以及 (b) 如果论文提供了信息，每位参与者的具体教育水平。

• **工业化**。我们使用各国的国内生产总值（GDP）作为衡量国民经济发展与进步最具代表性的指标 [56]。为了调整各国之间购买力的差异，我们采用基于购买力平价（PPP）的国内生产总值 [38]。

• **富裕程度**。我们通过分析两个指标，对参与者的财富进行了全面考察：(a) 基于购买力平价（PPP）的国家国民总收入（GNI） [39] 以及 (b) 如果论文中提供了相关信息，则考察每位参与者的具体收入水平。

• **民主**。我们使用政治权利评级，该评级反映各国的民主程度，涵盖选举进程、政治多元主义与参与，以及政府运作 [47]。

按国家人口归一化。为了探究哪些国家相对于人口而言，在 UPS论文中代表不足或过度，我们根据各国人口对参与者样本数量和参与者数量进行了归一化 [71]。具体而言，我们按如下方式计算参与者样本的归一化比率（ψ_s）和参与者的归一化比率（ψ_p）：

$$\psi_s = \frac{n_{samples}\,(\text{country}) \;\cdot\; \text{population (world)}}{n_{samples}\,(\text{total}) \;\cdot\; \text{population (country)}},$$

$$\psi_p = \frac{n_{participants}\,(\text{country}) \;\cdot\; \text{population (world)}}{n_{participants}\,(\text{total}) \;\cdot\; \text{population (country)}}$$

ψ_s 和 ψ_p 的值均不小于 0。$\psi_s < 1$或 $\psi_p < 1$ 的值表示该国代表不足，而 $\psi_s > 1$ 或 $\psi_p > 1$ 的值则表示，相对于该国人口占世界人口的比例，该国代表过度。例如，$\psi_s = 2$表示相对于该国人口，该国的研究关注度是其人口占比的两倍。

相关性分析。为了了解参与者样本在多大程度上来自EIRD国家，我们计算了 ψ_s 与各项 EIRD 指标（例如平均受教育年限和国内生产总值）之间的肯德尔秩相关系数。例如，如果 ψ_s 与平均受教育年限之间存在显著正相关，我们便可得出结论：UPS论文的参与者样本通常来自受教育程度较高的国家。

作者多样性。我们根据每位作者最先列出的隶属机构，确定了其所属机构所在的国家。

表6：参与者样本和参与者的数量。

国家	样本数		参与者人数	
	我们的方法	[61]	我们的方法	[61][4]
西方	624	1,102	183,828	174,041
非西方	167	405	38,208	75,068
报告为“其他”	–	–	4,836	n/a
% 西方	78.89%	73.13%	82.79%	69.87%

每篇论文均被归类为仅有具有西方背景的作者、同时包含具有西方背景的作者和隶属于非西方机构的作者，或仅有隶属于非西方机构的作者。

会议和研究主题之间的差异。为了揭示会议的特征，我们比较了各会议中仅由西方隶属机构作者发表的论文比例、仅招募西方参与者样本的论文比例，以及报告参与者所在国家的论文比例。同样，我们还比较了不同研究主题、参与者类型、设计评估（是/否）和攻击可行性评估（是/否）下的这些比例。

4 结果

4.1 西方

在我们的数据集中，51.89%（371/715）的论文明确报告了参与者所在国家。在 15.94%（114/715）的论文中，尽管作者没有提及参与者所在国家，但我们能够根据作者的隶属机构推断出来（例如，作者提到参与者是在当地招募的，且所有作者所在机构都位于同一个国家）。对于其余 32.17%（230/715）的论文，由于作者没有提供相关描述或描述不清，我们无法有把握地确定参与者所在国家。例如，有些论文：（i）只说明参与者是在当地招募的，或用户研究是当面进行的，但并非所有作者都在同一个国家；（ii）只说明参与者是通过社交媒体、众包或个人联系人招募的（即这些招募方法可能涵盖作者所在国家以外的人，尤其是在线研究）；（iii）只说明参与者是在某个国家举办的安全会议上招募的（部分参会者可能来自该国以外）。我们在附录A.3中提供了参与者所在国家编码流程图。

表 6 展示了我们能够识别或推断出参与者所在国家的 485 篇论文中的参与者样本数量和参与者人数。就参与者样本数量而言，绝大多数 UPS论文涉及西方参与者样本（78.89%，624/791）。这一比例高于 Linxen研究中 [61] 对人机交互领域研究进行审查所得的结果（73.13%）。就

[4] Linxen研究中未提及此数值，但我们根据作者发布的实验产物数据整理得出了该数值。

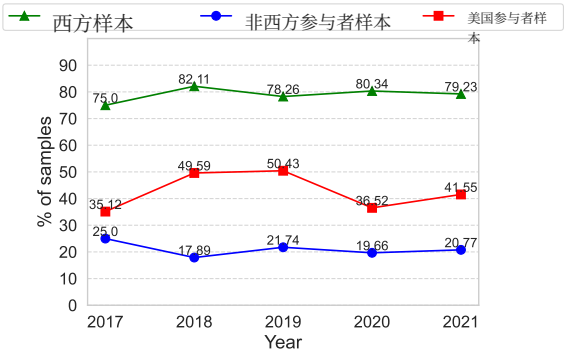

图 1：参与者样本的时间变化。

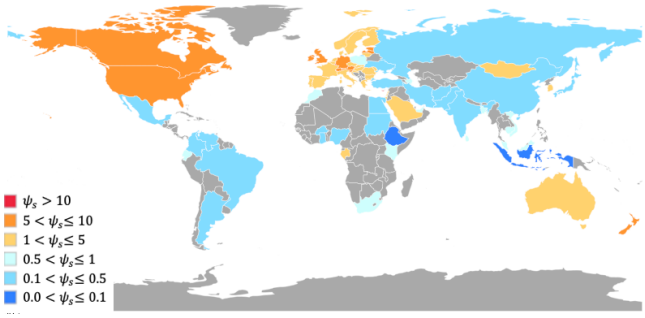

图 2：标准化参与者样本的分布。

参与者数量方面，共有226,872名参与者参与了UPS用户研究。除去4,836名被报告为“and other”且其详细信息不可用的参与者外，82.79%（183,828/222,036）的参与者来自西方国家。尽管我们的分析方法与Linxen研究中的方法相同 [61],请注意，这是一个保守估计，因为我们只纳入了能够识别或推断参与者所在国家的论文。如果研究人员招募了非西方人，他们很可能会对此进行报告，因为这是一种不常见的做法。因此，我们担心西方参与者样本的真实比例要高得多。

图 1 展示了五年期间西方、非西方和美国参与者样本占比的时间变化。Linxen研究报告称，2016–2020年间，CHI论文中非西方参与者样本的占比大幅增加（16.31%至30.24%，1.85倍）；而我们的结果显示，2017–2021年间，UPS论文中的该占比略有下降（25.00%至20.77%，0.83倍）。

表 7展示了参与者样本数量排名前五的国家、按国家人口归一化的参与者样本比率，以及参与者数量，从而帮助我们了解哪些国家被过度代表或代表不足。参与者样本按国家人口和参与者数量分布，UPS论文的参与者样本明显偏向四个西方国家：美国是最常被研究的国家，其次是德国、英国和加拿大。尽管这四个国家也与CHI论文（Linxen研究）中的排名前四国家相同，但它们在UPS论文中的占比（63.84%）高于CHI论文（55.61%）。考虑到美国人口占世界人口的比例，美国参与者样本在UPS领域中被过度代表了9.79倍。图 2 展示了参与者样本归一化比率的全球分布。2017年至2021年间，UPS论文中的参与者仅来自79个国家，许多国家完全未出现在这张地图中，尤其是非洲国家。南美洲、中东和亚洲也有许多国家缺失或代表不足。

在接下来的两个小节中，将分别分析 E、I、R 和 D 的指标。来自完全 WEIRD（即使用 AND 作为逻辑运算符）国家的参与者样本所占百分比见附录 B.

4.2 受教育程度

表8 展示了各国参与者样本的标准化比例与各国平均受教育年限之间的相关性（参见第3.2节中的教育分析（a））。我们发现二者呈正相关（r =.57，p <.001），也就是说，UPS论文中的大多数参与者样本都来自总体受教育程度较高的国家。

接下来，我们根据每篇论文中的详细描述，分析了参与者的教育水平（参见第 3.2 节中的“教育水平分析-(b)”）。在我们的数据集中，只有 34.69%（248/715）的论文明确报告了参与者的教育水平。尽管有 14.13%（101/715）的论文未报告参与者的教育水平，但由于作者提到招募了大学生，我们得以推断参与者的教育水平。其余 51.19%（366/715）的论文中，我们未能找到有关参与者教育水平的描述。在作者明确报告参与者教育水平的 248 篇论文中，71.38%（79,539/111,436）的参与者接受过大学或更高水平的教育，20.89%（23,282/111,436）接受过中等或更低水平的教育，其余 7.73%（8,615/111,436）则报告为“其他”或“不愿回答”。UPS论文中的参与者（71.38%接受过大学教育）与 CHI 论文中的参与者（69.93%接受过大学教育）受教育程度相当高。我们认为，参与者教育水平偏高与招募方法有关（见第 4.4 节）：（1）许多论文从作者所在的机构（包括大学）招募参与者；（2）许多论文通过众包招募参与者

[5]日本参与者样本数量较少（N=6），但其中一项用户研究招募了数量非常庞大的参与者（N=20,645）。

表7：按参与者样本数量（左）、参与者样本归一化比率（中）和参与者数量（右）排列的前五个国家。

按*nsamples*排名的国家				按Ψs排名靠前的国家				按参与者人数排名的国家			
国家	样本数量	%	Ψs	国家	样本数	%	Ψs	国家	参与者人数	%	Ψp
U.S.	329	41.59	9.79	安道尔	1	0.13	127.98	U.S.	142,908	62.99	14.83
德国	76	9.61	8.94	塞浦路斯	2	0.25	16.33	日本[5]	21,979	9.69	5.97
UK	67	8.47	9.73	卢森堡	1	0.13	15.77	德国	21,857	9.63	8.96
加拿大	33	4.17	8.61	奥地利	9	1.14	9.85	UK	9,297	4.10	4.71
印度	26	3.29	0.19	U.S.	329	41.59	9.79	中国	4,994	2.20	0.12

表 8：参与者样本归一化比率Ψs与受教育、工业化、富裕和民主各项指标的相关性。

指标	r	r [61]
受教育程度（平均受教育年限）	.57***	.46***
工业化（国内生产总值）	.49***	.50***
富裕（国民总收入）.52***		.50***
民主（政治权利）.44***		.50***

显著性水平：*$p < .05$，**$p < .01$，***$p < .001$。

例如 MTurk（例如，MTurk 工作者的受教育程度往往高于美国普通人口 [82]）；（3）有一定比例（14.96%）的论文招募了专家（他们通常受教育程度较高）。

4.3 工业化、富裕与民主

表 8 展示了参与者样本的归一化比率与国家的国内生产总值和国民总收入之间的相关性结果（见第3.2节中关于富裕（a）的分析）。我们发现，国内生产总值（r =.49，p <.001）和国民总收入（r =.52，p <.001）均呈正相关，也就是说，UPS论文的大多数参与者样本来自工业化且富裕的国家。

接下来，我们根据各篇论文中的详细描述分析了参与者的收入（见第 3.2节中关于富裕（b）的分析）。然而，只有5.59%（40/715）的论文报告了参与者的收入水平。与Linxen研究一样，我们也无法直接确定参与者的财富是否能代表总体人口。

最后，如表 8所示，我们发现参与者样本的归一化比率与国家的政治权利之间呈正相关（r =.44，p <.001），也就是说，UPS论文的大多数参与者样本来自政治权利方面自由度较高的国家。

4.4 作者多样性与方法论

在我们的数据集中，86.57%（619/715）的论文作者全部隶属于西方国家的机构，这一比例甚至略高于Linxen研究中的西方偏向（83.08%[6]）。9.93%（71/715）的论文的作者既有隶属于西方机构的，也有隶属于非西方机构的；其余3.50%（25/715）的论文作者则全部隶属于非西方机构。包含隶属于非西方国家机构作者的论文比例基本保持不变：从2017年的14.53%（17/117）到2021年的13.43%（27/201）。

表 9 展示了作者隶属机构所在国家、参与者所在国家、研究方法和招募方法之间的关系。在80.84%（464/574）的用户研究中，作者仅从其隶属机构所在国家招募参与者。正如我们在第 4.1 节中所述，参与者样本偏向西方国家的可能原因包括：（1）UPS论文中作者的隶属机构所在国家偏向西方国家；（2）作者倾向于在其隶属机构所在国家招募参与者。

在大多数用户研究中，通常会进行调查、访谈或实验室研究。如表 9 所示，当作者从其他国家招募参与者时，他们更有可能进行调查，而非实验室研究或访谈。实验室研究和访谈要求研究人员与参与者即时、互动地交流，因此语言障碍是一个严重的问题。此外，地理障碍也会影响研究方法的选择。实验室研究和访谈基本上要求参与者亲自前往特定位置，而调查在大多数情况下则在线进行。请注意，得益于视频会议服务，如今访谈也可以在线进行。

在作者所在国家招募参与者时，作者往往会在自己的机构内招募（在大多数用户研究中，这些机构是大学）。我们发现，众包平台常用于在作者所在国家内外招募参与者。不过，亚马逊土耳其机器人（MTurk）和 Prolific 等常用众包平台的注册工作者主要来自西方。具体而言，MTurk 工作者大多来自美国，其次是印度；而 Prolific 工作者主要来自英国，其次是美国和其他欧洲国家 [76, 79]。因此，这类热门平台对招募非西方人助益甚微。具体来说，得益于印度拥有大量 MTurk 工作者和英语使用者，印度参与者样本在我们的数据集中排名第五，如表 7 所示；但除印度外，西方作者较少研究其他非西方国家。

[6]Linxen研究中未提及此值，但我们使用作者发布的实验产物数据对其进行了汇编。

表 9：作者所属机构与研究/招募方法。

作者	参与者	研究方法		招募方法	
		调查	访谈/实验室	Top1	Top2
仅西方国家	仅作者所在国家 (72.65%)	35.73%	55.88%	机构 (32.85%)	计算机科学（27.58%）
	其他国家：仅西方国家（7.84%）	57.78%	37.78%	计算机科学（40.00%）	社交媒体（28.89%）
	其他国家：包括非西方国家（7.49%）	60.47%	32.56%	社交媒体（32.56%）	计算机科学（30.23%）
非西方包含	仅作者所在国家为西方国家（2.79%）	62.50%	31.25%	计算机科学（62.50%）	机构（12.50%）
	仅统计作者所在国家：包括非西方国家（5.40%）	25.81%	58.06%	机构（51.61%）	机器学习/个人计算机（22.58%）
	其他国家：仅西方国家（1.22%）	85.71%	14.29%	计算机科学 (85.71%)	机构 (14.29%)
	其他国家：包括非西方国家 (2.61%)	33.33%	53.33%	城市（26.67%）、机器学习/个人计算机（26.67%）	

我们展示的是用户研究的百分比，而非论文的百分比，因为一篇论文中可以开展多项用户研究（例如访谈和调查）。我们重点关注能够识别或推断参与者所在国家的用户研究。图中数值表示实线分隔的各部分中用户研究所占的百分比。“访谈/实验室”：访谈或实验室研究。“计算机科学”：众包。“机器学习/个人计算机”：邮件列表或个人联系人。

表10：会议的特征。

会议	% 国家已报告	% 攻击可行性	% W-only 作者	% 仅写入样本
S&P 领域	56.08 (36.86)	18.82	81.96	85.31
人机交互领域	75.83(61.25)	0.42	89.58	84.62
以 UPS 为重点	72.73(59.09)	0.45	88.64	86.25

“S&P 领域”：S&P、SEC、CCS、NDSS 和 PETS。“人机交互领域”：CHI 和 CSCW。“以 UPS 为重点”：SOUPS、EuroUSEC 和 USEC。“报告国家”列：我们能够识别或推断出参与者所在国家的论文百分比（括号中的数字表示我们能够识别出参与者所在国家的论文百分比）。

我们关注具有西方背景的作者如何招募非西方参与者（不包括通过 MTurk 容易招募到的印度人）。在这类用户研究中，作者会在社交媒体上发布研究招募信息；或者由一位隶属西方机构、但有非西方背景的作者负责在当地城市或通过其社交网络进行招募 [8, 9]。

4.5 会议之间的差异

表10 按会议展示了作者和参与者样本的特征。每个会议的作者隶属机构和参与者都偏向西方人。与人机交互会议（CHI 和计算机支持的协同工作）以及以用户隐私与安全为重点的会议（SOUPS、EuroUSEC 和 USEC）相比，作者明确报告参与者所在国家的论文比例，在 S&P、SEC、CCS、NDSS 和 PETS 中较低。这五个会议（S&P、SEC、CCS、NDSS 和 PETS）中，仅为展示所提出攻击的可行性而招募参与者的论文比例相对较高。

4.6 研究主题与方法论

表11 按参与者类型和研究目标，展示仅招募西方样本的用户研究比例。就参与者类型（即非专家或专家）而言，我们发现，在以下用户研究中，仅招募西方样本的比例较高

表11：参与者类型与研究目标之间的差异。

	% 研究	% 国家报告	% W-only 样本
参与者 – 非专家	85.04	70.67 (53.07)	85.38
参与者 – 专家	14.96	53.97 (38.10)	77.94
设计评估 – 是	39.55	68.47 (41.44)	83.78
设计评估 – 否	60.45	67.98 (56.97)	84.97
攻击可行性 – 是	7.01	44.07（15.25）	92.31
攻击可行性 – 否	92.99	69.99 (53.51)	84.12

我们展示用户研究的百分比，而非论文的百分比，因为作者可以在一篇论文中开展多项用户研究（例如，研究人员在第一项研究中招募非专家，在第二项研究中招募专家）。

表12：研究主题之间的差异。

主题	% 论文	% 国家报告	% 仅 W 样本
访问控制和隐私-隐私偏好	31.47	75.11（63.56）	90.53
身份验证	17.34	65.32 (33.06)	82.72
漏洞、恶意软件、和事件响应	13.43	56.25 (41.67)	77.78
总体	11.33	77.78（67.90）	85.71
隐私增强技术—技术	9.79	60.00 (45.71)	85.71
社会工程	6.29	75.56（64.44）	79.41
隐私侵害	5.45	76.92 (66.67)	80.00
其他	4.90	34.29（14.29）	91.67

我们展示论文所占的百分比，而非用户研究所占的百分比，因为即使一篇论文开展了多项用户研究，其研究主题也可以归入同一个编码。

其研究对象为非专家的用户研究中，非西方参与者的比例高于研究对象为专家的用户研究。这一结果受到以下事实的影响：（1）以专家为研究对象的用户研究中，超过 40%（40.48%）招募了“开发者”；（2）在招募开发者方面，具有西方背景的作者通过 Freelancer.com（许多非西方开发者在该平台注册）以及源代码仓库（例如 GitHub）和应用商店（例如谷歌 Play 商店）上公开的开发者联系方式，成功接触到了非西方开发者。然而，如果排除招募了开发者的用户研究，其余用户研究（例如招募了系统/网络管理员和安全专家的用户研究）的参与者则明显偏向于

高度依赖西方参与者样本（88.57%）。

比较进行了设计评估（例如，评估所提原型的可用性，或所提安全助推的有效性）的用户研究与未进行设计评估的用户研究后，我们发现两者在参与者样本的西方偏差程度上没有差异。

仅用于展示所提攻击可行性的用户研究占 7.01%（59/842）。对于这类用户研究，我们发现：（1）作者较少明确报告参与者所在国家（15.25%）；（2）作者倾向于只招募西方样本（92.31%）。攻击可行性研究中的参与者样本存在严重的西方偏差，这可以由以下事实解释：容易产生人口统计偏差的 MTurk 和实验室研究（例如，MTurk 工作者大多来自美国，而西方国家的大学研究人员很可能会招募本校学生参加实验室研究）常被用于展示攻击的可行性。我们进一步分析了攻击可行性研究（56 篇论文，包含 59 项用户研究），并确认在大多数研究中（54.24%，32/59），攻击可行性会受到参与者人口统计信息的影响。占多数的攻击有两类：（i）针对自动语音识别的攻击（15.25%，9/59）；（ii）打字／击键推断攻击（13.56%，8/59）。由于这类研究大多默认使用英语音频或英语输入，攻击可行性可能因参与者使用的语言而异。例如，英语水平较低的参与者可能难以识别恶意英语音频。此外，例如，各语言区域所使用的键盘布局和字符输入／转换方法会影响打字／击键推断的可行性。因此，展示攻击可行性的作者还应妥善报告参与者的人口统计信息，例如居住国和语言熟练度。

表 12 按研究主题展示了仅招募西方参与者样本的论文所占比例。在 UPS 领域，“访问控制与隐私偏好”是研究最频繁的主题，其次是“身份验证”、“漏洞、恶意软件和事件响应”以及“总体”。每个主题都普遍存在西方偏差。“访问控制与隐私偏好”和“其他”主题中的西方偏差相对更严重。另一方面，以下三个研究主题中的西方偏差相对较轻：(i) 在“漏洞、恶意软件和事件响应”主题中，研究人员经常招募开发者，且如上所述，研究人员成功招募到了非西方开发者；(ii) 在“社会工程”主题中，一些研究人员意识到调查非西方人（例如新兴市场国家公民 [81] 和非母语英语使用者 [42]）网络钓鱼易感性的重要性；(iii) 在“隐私侵害”主题中，研究人员经常关注少数群体和处境困难的人口群体所面临的隐私问题，其中一类群体是非西方人（例如，面临性别差距的非西方国家女性 [86]）。

5 讨论

我们的文献综述结果表明，UPS 的非西方参与者样本少于人机交互领域，而且非 WEIRD 参与者样本的比例略有下降。这意味着 UPS 领域应加大力度，解决这一地理多样性问题。基于我们的研究发现，我们提出了一些建议，以便进一步探索在地理分布更多元的人群中开展 UPS 研究。

5.1 主要发现摘要

我们的综述和分析的主要发现如下：

- 只有 51.89% 的 UPS 论文明确报告了参与者所在的国家。在非人机交互领域且非以用户隐私与安全为重点的会议上，作者报告这些信息的可能性较低。在我们能够识别或推断出相关信息的论文中，78.89% 的参与者样本来自西方。2017 至 2021年间，西方偏差有所加剧。（RQ1，第 4.1 和 4.5节）
- 参与者样本往往来自根据国家统计数据被认为具有较高教育水平、工业化程度高、富裕且民主的国家。明确报告参与者教育背景和/或收入水平的论文比例并不高。（RQ1，第 4.2 和 4.3节）
- 大多数 UPS论文（86.57%）的作者全部隶属于西方国家的机构。作者往往会从其隶属机构所在的国家招募参与者。当作者从其他国家招募参与者时，由于语言和地理障碍，他们更倾向于开展调查，而不是实验室研究或访谈。（RQ2，第4.4节）
- 具有非西方背景的作者、社交媒体，以及面向开发者的某些招募方法（例如源代码仓库和应用商店）都有助于招募非西方人。另一方面，关于专家（不包括开发者）的研究，以及旨在证明攻击可行性的研究，其参与者样本严重偏向西方参与者样本。（RQ2，第4.4节和4.6节）

5.2 面向非WEIRD人群的复现

重复研究可用于考察现有研究的发现能否推广至新的群体，也可用于评估在采用新的研究设计时，现有研究的发现是否具有稳健性。尽管有几项

现有的UPS论文已经表明，区域和文化差异会影响研究结果。 [44, 59, 88], 我们发现，大多数UPS论文仅考察了WEIRD国家，并未考虑或讨论地理多样性是否会影响研究结果。因此，研究人员在追求研究结果普遍适用性的同时，应探索来自地理分布多样化群体的不同见解。认识到群体差异，是解决边缘化群体所面临问题的一条有前景的途径。

复现研究被认为非常重要，专注于 UPS 的会议也对此予以推荐。例如，SOUPS 在征稿启事（CFP）中强调了复现研究的重要性 [2],，而 USEC 和 EuroUSEC 则将其列入征稿启事的主题。我们的数据集中有七篇复现论文 [15, 18, 19, 21, 28, 89, 104][7]。然而，当前的复现研究对非WEIRD人群关注不足；一些论文开展了跨文化复现，但仅限于西方国家。应积极开展兼顾地理多样性（包括非WEIRD人群）的复现研究，并在征稿启事中明确予以推荐。

程序委员会（PC）需要了解地理多样性所带来的区域、文化和机构差异，以便恰当地评估针对非 WEIRD 参与者的研究以及针对非 WEIRD 参与者的复现研究的价值。为此，仅有西方程序委员会成员可能不足以涵盖广泛的知识基础。换言之，程序委员会成员需要更多元化。我们还分析了 UPS 中程序委员会的多样性，发现程序委员会成员也大多偏向于隶属于西方国家机构的研究人员：2021年，在以用户隐私与安全为重点的会议（SOUPS、USEC 和 EuroUSEC）及研究专题（CHI 中的“隐私与安全”分委员会、CCS 中的“安全性、可用性与测量”专题）中，程序委员会成员大多是隶属于西方机构的研究人员（89.44%，127/142）。Soneji等人通过访谈顶级安全会议的程序委员会成员，揭示了评审流程中的挑战 [93]。尽管他们提到了程序委员会成员专业知识方面的问题，却没有讨论程序委员会成员缺乏地理多样性的影响。这表明，在顶级安全会议中，程序委员会成员的西方偏差目前尚未被充分认识为一个主要问题。与 UPS 相关的会议应开放程序委员会提名，并根据地理多样性遴选程序委员会成员。此外，丰富程序委员会多样性的另一种补充方法，是积极联系研究非西方（非 WEIRD）群体、并具备跨文化/区域研究专长的研究团队。作为第一步，这些研究团队不一定要有非 WEIRD国家背景，只要具备跨文化/区域研究专长和充分的文化知识即可。

[7]在我们的数据集中，我们将标题中包含“Replication:”的论文识别为复现论文。SOUPS 建议采用这一标题命名规则。

5.3 可复现性和参与者保护

可复现性较低的论文可能会阻碍复现研究。通过评审，我们发现许多论文存在可复现性问题，例如缺少用户研究参与者的基本人口统计信息。比如，我们能够确认参与者所在国家的论文比例并不够高（第4.1节），描述参与者教育或收入水平的论文比例也不够高（第4.2 节和4.3节）。此外，大多数攻击可行性研究都没有报告参与者人口统计信息，而这至关重要，因为许多攻击使用英语音频或输入，凸显了语言熟练度的影响（第4.6 节）。我们建议研究人员恰当报告参与者人口统计信息，这有助于开展复现研究的研究人员分析结果的普适性和群体差异。请注意，报告的所有参与者人口统计信息不一定都要逐一与研究结果关联，因为这种强行关联需要进行大量统计检验才能达到所需的p值，并会导致误导性解读（称为p值操纵）。

许多论文对参与者人口统计信息的描述分散在不同位置，因此研究人员（即这些论文的读者）可能需要花费大量时间查找相关描述。此外，许多论文虽然提供了一些信息，但描述不够清晰，也不充分（常见示例请参见第 4.1 节）。研究人员若要识别参与者人口统计信息的报告内容，一种直接的方法是采用清单或统一格式。例如，顶尖人工智能会议之一 NeurIPS 已推出一份用于人工智能研究可复现性的清单 [1]。此外，Distler等人建议 UPS研究人员采用自查格式，以便清晰了解用户研究中的风险呈现方式 [32]。然而，要识别和报告参与者人口统计信息，研究界需要更审慎地讨论这类做法，因为它可能 (i) 简化识别参与者人口统计信息时涉及的敏感问题，或 (ii) 对高风险群体的安全构成威胁。对于第一种情况，研究人员在识别某些人口统计信息时需要谨慎考虑，例如询问跨性别者其认定的性别，或询问生活在因冲突地区或领土争端而无法明确定义的地区的人其居住国。为避免这些问题，研究人员应提供充足的选项，以涵盖广泛的个体身份表达。对于第二种情况，研究人员需要采取措施，保护高风险群体（例如政治活动人士和亲密伴侣虐待或暴力幸存者）的人身与数字安全。Bellini等人总结了在研究前、研究中或研究后保护高风险群体隐私及人身与数字安全、避免其被重新识别的做法；具有代表性的做法包括省略研究程序和人口统计信息的细节 [17, 66]。因此，

UPS社区也需要了解，当参与者属于高风险群体时，不澄清与其身份相关信息的原因。

5.4 地理障碍

UPS论文中参与者样本偏向西方的现象，与大多数作者隶属于西方国家的机构这一事实有关；正如第 4.4 节所述，作者往往会从其隶属机构所在国家招募参与者。地理障碍可能会促使研究人员选择最方便的样本(例如，当地大学的学生，他们很容易被大学研究人员招募）。在线方法可作为克服地理障碍的一种有前景的途径。我们的结果表明，众包是从作者所在国家以外招募参与者的常见方式。不过，请注意，热门众包平台上的参与者群体也存在偏向。尽管 MTurk、Prolific 和 Clickworker 等众包平台常被用于招募作为终端用户的参与者，但这些平台上的工作者基本都来自西方，研究人员无法触及居住在西方以外地区的人，例如亚洲国家和全球南方的人。因此，为克服上述参与者招募中的地理障碍，研究人员应考虑使用目标人群所在国家使用的本地（区域性）众包平台。另一方面，在线方法有一个主要缺点：只有能够接入互联网且对信息技术有一定了解的人才能参与。在全球南方，这一问题更加严重。作为补充解决方案，我们建议提高研究者多样性，并加强与本地研究者的合作，正如第5.5节所述。

通过众包招募专家通常比招募非专家（终端用户）更困难。这是因为在众包平台注册的大多数工作者都是非专家。即使如此，研究人员仍经常在线招募软件开发人员，例如通过 Freelancer.com（面向自由职业开发者的众包平台）、源代码仓库（如 GitHub）中的联系人列表，以及应用商店（如 Google Play 商店）；第 4.6 节对此有所提及。然而遗憾的是，据报道，目前招募软件开发人员的方法存在若干合同和方法方面的问题。Danilova 等人于 2021 年发表的研究中承认，Freelancer.com 拒绝了他们面向软件开发人员开展用户研究的学术任务 [30]。这意味着研究人员的“学术”目标与平台的“商业”目标不匹配。此外，一些研究人员开始从源代码仓库、应用商店和社交媒体收集开发者的电子邮件地址，以此招募软件开发人员；Tahaei 等人指出，目前并不支持通过收集这些平台上的信息来进行大规模招募（至少在 GitHub 上，这种收集行为违反服务条款和隐私政策） [98]。此外，Danilova 等人和 Tahaei 等人指出，在线招募往往会纳入开发技能不足以参与用户研究的软件开发人员，并评估了用于核实参与者是否具备足够开发技能的筛选方法 [27,29,98]。

通过在线方法（例如众包、源代码仓库、应用商店和社交媒体）招募专家的研究大多聚焦于软件开发人员。然而，UPS研究中的专家群体更加多样，不仅限于软件开发人员，还包括系统／网络管理员、SOC分析师、安全专家等。由于当前众包平台的参与者群体中很难找到这类专家，因此招募方法往往依赖个人联系人。虽然目前还没有针对软件开发人员以外的专家的突破性招募方法，但人们希望能有一个不受地理或语言障碍限制、并通过激励吸引专业人士的平台。

5.5 语言障碍

上一节提到的在线研究能够（部分）消除招募过程中的地理障碍，但研究非 WEIRD 群体也面临语言障碍。我们建议通过以下方式减少 UPS 研究中的语言障碍：（1）提升作者的地理多样性；（2）赋能非西方研究人员。

尽管许多国家将英语作为国家语言，但非英语母语者占世界人口的大多数，而且许多国家的英语水平并不够高 [33]。不同国家使用不同语言所造成的语言障碍，会显著影响单一语言社群内部研究的本地化（第4.4节）。以下两种情况会显现出语言障碍：（1）参与者与研究人员，以及（2）文档与研究人员使用不同的母语。对于第一种情况，即参与者与研究人员使用不同母语，尤其是在需要即时沟通的用户研究中，研究人员难以向参与者准确传达研究意图，也难以理解参与者回答所表达的意思。事实上，第4.4 节的结果表明，从其他国家招募参与者时，作者更可能开展调查，而非实验室研究或访谈。Dell等人评估了本地访谈员与外国研究人员借助翻译人员开展访谈时，需求特征所导致的参与者反应偏差差异 [31]。结果表明，相较于本地访谈员，外国研究人员引发的实验产物偏差更大。因此，难以与使用其他语言的人进行访谈，可能是包括UPS在内的人因研究面临的严重问题。对于第二种情况，即文档与研究人员使用不同母语，尽管理解在线公共建议、政策（例如隐私

政策）以及社交媒体上的用户帖子[8] 是UPS领域的重要工作，但研究人员难以正确分析以外语撰写的此类文档。Redmiles等人指出，在通过大规模分析网络上的建议来确定安全与隐私建议的优先级时，关键挑战在于 [83], , 由于收集的建议来自MTurk工作者（主要是包括美国在内的英语国家工作者），所得结果不可避免地仅限于英语建议。在对在线网络钓鱼建议的分析中，Althobaiti等人明确指出了语言方面的局限；为避免过度依赖自动翻译，他们将调查范围限定在少数国家的网页 [13]。英语使用者研究人员在非英语国家开展研究时，最好与以该国所用语言为母语的研究人员合作。从非英语国家的研究视角来看，尤其是在全球南方，研究人员可能需要额外付费，将参与者的回答或文档翻译成发表所用的语言（即英语）。为减少这些语言障碍，UPS 研究群体应促进跨国合作署名，并考虑提供语言支持，包括分摊费用。

会议地点多样化不仅有望通过增加多元化会议参会者的数量来促进研究人员之间的合作 [67]，还可通过激活本地研究社群并推动技术转移，培育和壮大本地（例如，非西方）研究人员。然而，在 UPS 领域，大多数会议都在有限的地点举办。S&P、NDSS 和 SOUPS 从未在美国以外举办过；USENIX Security 大多在美国举办，仅有一次在加拿大举办；CCS 几乎只在美国和欧洲举办（仅在 2021年 于韩国举办过一次）。

5.6 研究正义考量

研究正义是一种理念和方法，旨在阐明并确保研究中的公平、公正和伦理考量，尤其是在包括非 WEIRD 人群在内的社区合作中。它关注权力失衡，促进包容性，并尊重边缘化群体或个人的权利与利益。Haelewaters 等人批评了“直升机式研究”，即全球北方（即较富裕的全球化国家，如西方国家）的研究人员往返于全球南方开展研究，却几乎不让本地合作者参与，并指出这是损害研究正义的典型例子 [41]。Haelewaters 等人提出了避免直升机式研究的规则，以促进全球北方与全球南方之间更优质、更具协作性且非殖民化的科学研究。这些规则主要包括与本地研究人员进行平等且协同增效的合作，按照伦理和公平原则对待发表与作者署名，认识到工作文化的差异，以及使用本地基础设施。这些规则也与我们的建议相关：提高研究人员的多样性并加强与本地研究人员的合作（第 5.4和 5.5节），通过促进本地研究社区发展和技术转移来培养并加强本地研究人员（第 5.5节），提高程序委员会成员的多样性，吸纳了解非 WEIRD 社会／人群的成员（第 5.2节），以及使用本地众包平台（第 5.4节）。在推动关于非 WEIRD 社会／人群的研究时，UPS社区需要将 Haelewaters 等人的规则作为研究原则加以遵循。

5.7 未来研究

在第 2.2 节中，我们介绍了 WEIRD 偏倚会如何损害 UPS 研究。在此，我们基于文献综述，探讨 USP 未来研究中具有潜力的方向，并重点指出尚未披露的事实和亟待解决的挑战。

WEIRD视角。我们的结果表明，参与者样本偏向于受教育、工业化、富裕和民主（EIRD）国家，也偏向西方国家。关于“西方”，我们发现 UPS论文无论研究何种主题，都存在西方偏差。在这些论文中，研究专家（开发者除外）的参与者样本尤其偏向西方人。正如第4.6节所述，尽管聚焦开发者的论文在一定程度上研究了非西方参与者样本，但专家群体更多样，涵盖系统/网络管理员、SOC分析师和CSIRT工程师。在软件开发领域，各国的组织结构各不相同，因此产生了不同的组织约束 [52]。这表明，研究非西方国家中各类专家所面临的组织与文化问题，是一个很有前景的研究方向。关于“受教育”，仅研究受教育程度高的国家并不足够，因为全球南方国家在网络安全教育发展方面面临诸多挑战。全球南方的网络安全教育总体上仍处于初级阶段 [23],, 而且研究发现，个体参与者的教育水平是普遍影响其安全与隐私行为的重要因素 [77, 107, 113]。研究人员应明确全球南方的人们接受何种安全与隐私教育和建议，并努力缩小全球南方与全球北方在安全与隐私教育方面的数字鸿沟。关于“工业化”和“富裕”，一些研究已关注全球南方人们的安全与隐私顾虑；这些地区的人们 IT资源有限，例如面临设备共享相关的顾虑，而研究人员也为他们开发了支持技术 [10, 16, 85]。研究人员应调查支持技术能否在工业化和财富水平较低的其他国家和地区发挥实际作用。关于“民主”，

[8]仅分析在线公共数据、未开展用户研究的论文不在我们的文献综述范围内。

一些研究指出，政治自由度较低国家的人们对隐私的理解与其他国家的人们有所不同 [111]。这种民主差异可能会影响“访问控制与隐私偏好”这一主题的研究结果：正如第4.6节所述，该主题的参与者样本尤其偏向西方人。在政治高压政权下对潜在参与者开展用户研究时，研究人员应考虑并克服招募方法和研究方法上的困难，同时还要关注参与者可能因批评政府而面临风险这一伦理问题。第5.3节介绍了保护此类高风险参与者的研究实践。

设计评估。尽管 UPS 领域已开展了一些关于用户认知、关注点和实践的跨文化比较，但设计评估方面的研究仍然不足。在人机交互和心理学领域，众所周知，用户对界面设计和框架效应的偏好因国家而异 [51, 62, 70]；因此，应进一步识别不同国家在安全／隐私界面的可用性以及框架效应的有效性方面存在的差异，例如通知中的文本和图标如何鼓励用户采用安全技术，从而设计出适合各国用户的界面。

更多样化的非 WEIRD 社会/人群。拓展地理多样性是推动 UPS 研究发展的关键因素；然而，以非西方参与者样本所占比例作为衡量指标存在一个缺陷。如果有更多论文研究印度和中国（这两个国家已有一定程度的研究，参与者样本数量分别排名第五和第六），非西方参与者样本的比例就会提高；然而，过去五年里，非洲、南美洲和亚洲仍有许多非西方国家尚未得到研究（请参见第4.1节）。UPS 研究群体应努力了解更多样化的国家。

5.8 局限性

测量误差。 虽然人工分析中不可避免地会出现一些测量误差，但我们已尽可能清晰地描述文献综述流程，以确保编码的准确性。我们的数据集将在研究人员提出请求后提供，以提高可复现性并促进对我们研究的重复验证。

会议覆盖范围。 我们的数据集（十个会议，N=715）远大于近期关于 UPS 的代表性文献综述论文所涵盖的范围（五个会议，N=284 于 [32]）。我们的数据集涵盖了顶级且竞争激烈的会议，UPS 论文会在这些会议上发表，并且这些会议对全球众多研究人员和社群产生深远影响。了解此类会议中的 WEIRD 偏倚，是合理的第一步。请注意，关于非 WEIRD国家的论文也会在区域性会议（例如 AfriCHI）上发表，而这些会议并未纳入我们的数据集。

排除分析在线公共数据的论文。我们聚焦于作者招募参与者开展用户研究的UPS论文，而没有聚焦于作者分析在线公共数据的UPS论文。我们担心，此类UPS论文也偏向于西方社会，即研究人员调查了在西方在线服务上实施的设计和政策，以及西方用户发布的在线内容。

WEIRD框架的局限性。WEIRD框架的大多数指标[9] 假设每个国家的代表性人口人口统计数据。然而，一般而言，同一国家内的人各不相同。例如，即使参与者来自贫困国家，他们个人也可能很富有。此外，在线方法可以轻松招募具有互联网接入能力并且对信息技术有一定熟悉度的人，如第 5.4 节所述。此外，西方国家的低收入人群对于UPS社区仍然很有价值。然而，由于很少有论文报告参与者的收入水平，我们无法量化关于这类人群的论文数量。

多样性维度的其他指标。WEIRD 的五项指标只是人因研究中所考虑的多样性维度的一部分 [45]。UPS 研究人员应考虑 WEIRD 之外的各种多样性。例如，霍夫斯泰德的文化维度框架包含了一些很有前景的指标。我们还根据该框架对数据集进行了分析（请参见附录 C）。未来的研究需要全面捕捉影响 UPS 研究的多样性。

6 结论

本研究旨在了解可用隐私与安全（UPS）领域中招募参与者的地理多样性，以及研究方法和研究主题的特征。通过对715篇UPS论文进行全面的文献综述，我们发现，UPS论文的参与者样本高度偏向西方参与者（78.89%）。遗憾的是，这一偏向程度高于人机交互（HCI；73.13%）。此外，2017–2021年间，UPS论文中非西方参与者样本的比例有所下降（从25.00%降至20.77%，为0.83倍）。这表明，UPS领域应投入更多努力来应对这一地理多样性问题。我们提出了使UPS研究减少WEIRD（西方、受教育、工业化、富裕和民主）特征的建议：促进复现，处理研究和招募方法中的地理与语言问题，并确定未来的研究主题。我们希望，我们的发现和建议能够激励不断发展的UPS社区进一步实现多样化并增强包容性。

[9] E 和 I 的指标 同时使用国家平均值和个人 数据。

致谢

我们谨向原研究（Linxen研究）的作者Sebastian Linxen表示感谢， [61],感谢他为我们的复现工作提供建议。我们也感谢匿名评审员和指导编辑富有洞察力且 invaluable 的反馈。

参考文献

[1] NeurIPS 2021年。论文清单指南。 https://neurips.cc/Conferences/2021/PaperInformation/PaperChecklist，（访问于2022年8月2日）。

[2] SOUPS 2022年。征稿启事。 https://www.usenix.org/conference/soups2022/call-for-papers，（访问于2022年8月2日）。

[3] Noura Abdi、Xiao Zhan、Kopo M. Ramokapane 和 Jose Such。智能家居个人助理的隐私规范。载于*2021*年计算机系统中的人为因素*CHI*会议论文集，2021年。[4] Ruba Abu-Salma、M. Angela Sasse、Joseph Bonneau、Anastasia Danilova、Alena Naiakshina 和 Matthew S mith。采用安全通信工具的障碍。载于第*38*届*IEEE*安全与隐私研讨会论文集，2017年。[5]Mark S. Ackerman。计算机支持的协同工作的智力挑战：社会需求与技术可行性之间的鸿沟。人机交互，15(2)：179–203，2000。[6] Alessandro Acquisti、Idris Adjerid、Rebecca Balebako、Laura Brandimarte、Lorrie Faith Cranor、Saranga Komanduri、Pedro Giovanni Leon、Norman Sadeh、Florian Schaub、Manya Sleeper、Yang Wang 和 Shomir Wilson。隐私与安全助推：理解并协助用户进行在线选择。*ACM*计算调查，50(3)：1–41，2017年。[7] Anne Adams 和 Martina Angela Sasse。用户不是敌人。*ACM*通信，42(12)：40–46，1999年。[8] Syed Ishtiaque Ahmed、Md Romael Haque、Jay Chen 和 Nicola Dell。孟加拉国共享手机使用带来的数字隐私挑战。人机交互，1(CSCW)：1–20，2017年。[9] Syed Ishtiaque Ahmed、Md Romael Haque、Shion Guha、Md Rashidujjaman Rifat 和 Nicola Dell。全球南方的隐私、安全与监控：孟加拉国生物识别移动 SIM 卡注册研究。载于*2017*年计算机系统中的人为因素*CHI*会议论文集，2017年。

[10] Syed Ishtiaque Ahmed、Md Romael Haque、Irtaza Haider、Jay Chen 和 Nicola Dell。“每个人都有一些私人物品”：通过设计支持孟加拉国共享手机使用中的数字隐私。载于*2019*年计算机系统中的人为因素*CHI*会议论文集，2019年。

[11] Elham Al Qahtani、Yousra Javed、Heather Lipford 和 Mohamed Shehab。保守社会中的女性会（不）遵循智能手机安全建议吗？沙特阿拉伯和巴基斯坦的案例研究。载于第五届欧洲可用安全研讨会论文集，2020年。

[12] Kholoud Althobaiti、Nicole Meng 和 Kami Vaniea。我不需要专家！让 URL 钓鱼特征通俗易懂。载于*2021*年 *CHI* 计算系统人因会议论文集，2021年。

[13] Kholoud Althobaiti、Ghaidaa Rummani 和 Kami Vaniea。《人类与计算机侧 URL 钓鱼特征综述》。载于第*4*届欧洲可用安全研讨会论文集，2019年。[14] Jeffrey J. Arnett。《被忽视的95%：为什么美国心理学需要变得不那么美国化》。美国心理学家，63(7):602–614，2008年。[15] Khadija Baig、Elisa Kazan、Kalpana Hundlani、Sana Maqsood 和 Sonia Chiasson。《复现：媒体对技术用户心智模型的影响》。载于第*17*届可用隐私与安全研讨会论文集，2021年。[16] Khaled Baqer、Ross Anderson、Jeunese Adrienne Payne、Lorna Mutegi 和 Joseph Sevilla。《DigiTally：为手机试点离线支付》。载于第*13*届可用隐私与安全研讨会论文集，2017年。[17]Rosanna Bellini、Emily Tseng、Noel Warford、Tara Matthews、Alaa Daffalla、Sunny Consolvo、Jill Palzkill Woelfer、Patrick Gage Kelley、Michelle L. Mazurek、Dana Cuomo、Nicola Dell 和 Thomas Ristenpart。《SoK：涉及高风险用户的更安全数字安全研究》。*arXiv:2309.00735*，2023年。[18] Karoline Busse、Julia Schäfer 和 Matthew Smith。《复现：没人能入侵我的思想——重新审视一项关于专家与非专家安全实践及建议的研究》。载于第*15*届可用隐私与安全研讨会论文集，2019年。[19] Karoline Busse、Dominik Wermke、Sabrina Amft、Sascha Fahl、Emanuel von Zezschwitz 和 Matthew Smith。《复现：如果我们不会输，我们还会打瞌睡吗?

在习惯化用户研究中利用激励对风险进行建模。载于*2019*年可用安全研讨会论文集，2019年。

[20] Marcus A. Butavicius、Kathryn Parsons、Malcolm R. Pattinson、Agata McCormac、Dragana Calic 和 Meredith Lillie。理解易受钓鱼邮件影响的程度：评估个体差异与文化的影响。载于第 *11* 届国际信息安全与保障中的人类因素研讨会论文集，2017。

[21] Casey Canfield、Alex Davis、Baruch Fischhoff、Alain Forget、Sarah Pearman 和 Jeremy Thomas。复现：使用数据日志验证钓鱼检测能力指标所面临的挑战。载于 第*13*届可用隐私与安全研讨会论文集，2017年。[22] Weicheng Cao、Chunqiu Xia、Sai Teja Peddinti、David Lie、Nina Taft 和 Lisa M Austin。关于用户行为、预期以及对 Android 权限参与度的大规模研究。载于 第*30*届*USENIX*安全研讨会论文集，2021年。[23] Frankie E. Catota、M. Granger Morgan 和 Douglas C. Sicker。发展中国家的网络安全教育：厄瓜多尔环境。《网络安全期刊》，5(1)，2019年。[24] Giacomo Chiozza。是否存在文明冲突？国际冲突参与模式所提供的证据，1946—1997年。《和平研究杂志》，39(6)：711–734，2002年。[25] Sophie Cockcroft 和 Saphira Rekker。文化与信息隐私政策之间的关系。《电子市场》，26(1)：55–72，2016年。[26] comforte AG。17个拥有类似《通用数据保护条例》数据隐私法律的国家。
https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws，（访问于2023年6月2日）。[27]Anastasia Danilova、Stefan Horstmann、Matthew Smith 和 Alena Naiakshina。测试面向程序员的在线调查筛选问题中的时间限制。载于 第*44*届软件工程国际会议论文集，2022年。[28]Anastasia Danilova、Alena Naiakshina、Johanna Deuter 和 Matthew Smith。复现：在线安全开发者研究的生态效度：与自由职业者开展密码存储研究，探索欺骗问题。载于 第*16*届可用隐私与安全研讨会论文集，2020年。

[29]Anastasia Danilova、Alena Naiakshina、Stefan Horstmann 和 Matthew Smith。你真的会编程吗？为面向程序员的在线调查设计并评估筛选问题。载于 第*43*届软件工程国际会议论文集，2021年。

[30] Anastasia Danilova、Alena Naiakshina、Anna Rasgauski 和 Matthew Smith。将代码审查作为在线安全研究的方法论——以自由职业者的密码存储为例。载于第 *17* 届可用隐私与安全研讨会论文集，2021年。

[31] Nicola Dell、Vidya Vaidyanathan、Indrani Medhi、Ed- ward Cutrell 和 William Thies。“你的更好！”：人机交互中的参与者反应偏差。载于 *2012*年*SIGCHI*计算机系统中的人为因素会议论文集，2012年。[32] Verena Distler、Matthias Fassl、Hana Habib、Katharina Krombholz、Gabriele Lenzini、Carine Lallemand、Lorr- rie Faith Cranor 和 Vincent Koenig。可用隐私与安全研究中实证方法及风险表征的系统性文献综述。*ACM*计算机-人机交互汇刊，28(6):1–50，2021年。[33] EF英孚教育。EF英语熟练度指数。https://www.ef.com/wwen/epi/，（访问于2022年8月12日）。[34] Joseph L. Fleiss、Bruce Levin 和 Myunghee Cho Paik。评定者间一致性的测量。率与比例的统计方法，2(212-236):22–23，1981年。[35] Anjuli Franz、Verena Zimmermann、Gregor Albrecht、Katrin Hartwig、Christian Reuter、Alexander Benlian 和 Joachim Vogt。SoK：海里的“钓鱼”仍然很多——面向用户的网络钓鱼干预措施分类体系及未来研究方向。载于 第*17*届可用隐私与安全研讨会论文集，2021年。[36] George Fujii、Andrew Szarejko 和 Diane Labrosse。国际关系课堂中的文明冲突。
https://network.h-net.org/node/28443/discussions/5273269/h-diploissf-teaching-roundtable-11-6-clash-civilizations-ir，（访问于2022年11月27日）。[37] Simson Garfinkel 和 Heather Richter Lipford。可用安全：历史、主题与挑战。信息安全、隐私与信任综合讲座，5(2):1–124，2014年。

[38] 世界银行集团。人均国内生产总值，购买力平价（现价国际元）（2020年）。https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD。

[39] 世界银行集团。人均国民总收入，购买力平价（当前国际元）（2020年）。https://data.worldbank.org/indicator/NY.GNP.PCAP.PP.CD。

[40] Guofei Gu。计算机安全会议排名与统计。https://people.engr.tamu.edu/guofei/sec_会议_统计.htm，（访问于2022年8月18日）。

[41] Danny Haelewaters、Tina A. Hofmann 和 Adriana L. Romero-Olivares。全球北方研究人员停止在全球南方 perpetuating 直升机式研究的十条简单规则。*PLoS*计算生物学，17(8)，2021年。

[42] Ayako A. Hasegawa、Naomi Yamashita、Mitsuaki Akiyama 和 Tatsuya Mori。他们为何忽略英语邮件：非母语者识别网络钓鱼邮件所面临的挑战。载于第*17*届可用隐私与安全研讨会论文集，2021年。

[43] Joseph Henrich、Steven J. Heine 和 Ara Norenzayan。世界上最奇怪的人？行为与脑科学，33(2-3)：61–83，2010年。[44] Franziska Herbert、Steffen Becker、Leonie Schaewitz、Jonas Hielscher、Marvin Kowalewski、Angela Sasse、Yasemin Acar 和 Markus Dürmuth。一个充满隐私与安全（误）观念的世界？12个国家代表性调查的发现。载于*2023*年计算机系统中的人为因素*CHI*会议论文集，2023。[45] Julia Himmelsbach、Stephanie Schwarz、Cornelia Ger-denitsch、Beatrix Wais-Zechmann、Jan Bobeth 和 Manfred Tscheligi。我们是否关注人机交互中的多样性：关于研究中多样性维度的综合内容分析。载于*2019*年计算机系统中的人为因素*CHI*会议论文集，2019。[46] Geert Hofstede。文化维度化：情境中的霍夫斯泰德模型。心理学与文化在线读物，2(1)：2307–0919，2011年。[47] 自由之家。《世界自由度》（2020年）。https://freedomhouse.org/report/freedom-world。

[48] Samuel P. Huntington。《文明冲突与世界秩序的重建》。西蒙与舒斯特，2011年。

[49] Enzuzo公司。2023年的数据隐私法：你需要了解的规则与法规。https://www.enzuzo.com/blog/data-privacy-laws，（访问于2023年6月2日）。

[50] Hofstede Insights。国家比较工具。https://www.hofstede-insights.com/，（访问于2022年8月2日）。

[51] Jainaba Jagne 和 Serengul Smith。跨文化界面设计策略。《普适访问信息社会》，5:299–305，2006。

[52] Fumihiro Kanei、Ayako Akiyama Hasegawa、Eitaro Shioji 和 Mitsuaki Akiyama。关于软件开发项目安全工作与约束的跨角色、跨国分析。载于《第*37*届年度计算机安全应用大会论文集》，2021年。

[53] Mannat Kaur、Michel van Eeten、Marijn Janssen、Kevin Borgolte 和 Tobias Fiebig。安全研究中的人因：从2008—2018年汲取的经验。*arXiv:2103.13287*，2021年。[54] Nir Kshetri。非洲的网络犯罪与网络安全。《全球信息技术管理期刊》，22(2):77–81，2019。[55] Pedro Giovanni Leon、Blase Ur、Yang Wang、Manya Sleeper、Rebecca Balebako、Richard Shay、Lujo Bauer、Mihai Christodorescu 和 Lorrie Faith Cranor。用户看重什么？影响用户向在线广告商共享信息意愿的因素。载于《第*9*届可用隐私与安全研讨会论文集》，2013年。[56] Philipp Lepenies。《一个数字的力量：国内生产总值的政治史》。哥伦比亚大学出版社，2016年。[57] Ling Li、Wu He、Li Xu、Ivan Ash、Mohd Anwar 和 Xiao-hong Yuan。探究网络安全政策意识对员工网络安全行为的影响。《国际信息管理期刊》，45:13–24，2019年。[58] Yao Li、Reza Ghaiumy Anaraky 和 Bart Knijnenburg。如何正确测量社交网络隐私：一项跨国调查。《人机交互》，5(CSCW):1–32，2021年。[59] Yao Li、Alfred Kobsa、Bart P. Knijnenburg 和 M-H Carolyn Nguyen。跨文化隐私预测。载于《第*17*届隐私增强技术研讨会论文集，PETS'17，2017年。

[60] Yifang Li、Nishant Vishwamitra、Bart P. Knijnenburg、Hongxin Hu 和 Kelly Caine。混淆作为一种用于照片分享的隐私增强技术的有效性和用户体验。人机交互，1(CSCW)：1–24，2017。

[61] Sebastian Linxen、Christian Sturm、Florian Brühlmann、Vincent Cassau、Klaus Opwis 和 Katharina Reinecke。CHI有多WEIRD？载于*2021*年计算机系统中的人为因素*CHI*会议论文集，2021年。

[62] Aaron Marcus 和 Emilie West Gould。交汇：文化维度与全球网络用户界面设计。*Interactions*，7(4):32–46，2000。

[63] Diogo Marques、Tiago Guerreiro、Luis Carriço、Ivan Beschastnikh 和 Konstantin Beznosov。《脆弱性与归责：理解智能手机未经授权的访问》。载于*2019* 年 *CHI* 人因计算系统会议论文集，2019 年。

[64] Raima Mathew、Mutmaina Adebayo 和 Camille Cobb。《安全与隐私研究多样性的元分析》。载于第七届包容性隐私与安全研讨会论文集，2022年。

[65] Tara Matthews、Kathleen O'Leary、Anna Turner、Manya Sleeper、Jill Palzkill Woelfer、Martin Shelton、Cori Manthorne、Elizabeth F. Churchill 和 Sunny Consolvo。《幸存者的故事：应对亲密伴侣虐待时的隐私与安全实践》。载于*2017*年计算机系统中的人为因素*CHI*会议论文集，2017年。

[66] Jessica McClearn、Rikke Bjerg Jensen 和 Reem Talhouk。《被他者化、噤声并遭到污名：理解黎巴嫩边缘化群体的情境化安全》。载于第*32*届 *USENIX*安全研讨会论文集，2023年。

[67]Helena Mentis、Cliff Lampe、Regina Bernhaupt、Anirudha Joshi、Susan Fussell、Susan Dray、Dan Olsen、Aaron Quigley、Julie R. Williamson、Eunice Sari、Loren Terveen、Allison Druin 和 Philippe Palanque。《新一届SIGCHI执行委员会的价值观与战略举措》。*Interactions*，26(1):84–85，2018年。

[68] Sandra J Milberg、Sandra J Burke、H Jeff Smith 和 Ernest A Kallman。《价值观、个人信息隐私与监管方法》。*ACM*通讯，38(12):65–74，1995年。

[69] Alena Naiakshina、Anastasia Danilova、Eva Gerlitz 和 Matthew Smith。《如何开展安全开发者研究：对计算机科学专业学生、自由职业者和公司开发者开展密码存储研究》。载于*2020*年计算机系统中的人为因素*CHI*会议论文集，2020年。

[70] Yeseul Nam、Haeyoung Gideon Park 和 Young-Hoon Kim。《你是偏好正面信息，还是厌恶负面信息？框架效应推导中的文化差异》。*CurrentPsychology*，2021年。

[71] 联合国。《世界人口展望2019》（2020年估算）。https://population.un.org/wpp/DataQuery/。

[72] 美国国家标准与技术研究院。NIST SP-800 系列。https://csrc.nist.gov/publications/sp800，（访问日期：2023年6月2日）。

[73] Midas Nouwens、Ilaria Liccardi、Michael Veale、David Karger 和 Lalana Kagal。《通用数据保护条例》之后的暗黑模式：抓取同意弹窗并展示其影响。载于*2020*年 *CHI* 人因计算系统会议论文集，2020年。

[74] Borke Obada-Obieh、Yue Huang、Lucrezia Spagnolo 和 Konstantin Beznosov。《SoK：技术在性虐待中的双重属性》。发表于第*43*届*IEEE*安全与隐私研讨会论文集，2022年。

[75] Daniela Oliveira、Harold Rocha、Huizi Yang、Dono- van Ellis、Sandeep Dommaraju、Melis Muradoglu、De- von Weir、Adam Soliman、Tian Lin 和 Natalie Ebner。《剖析针对老年人与青年人的鱼叉式网络钓鱼邮件：影响力武器与生活领域在预测网络钓鱼易感性方面的相互作用》。发表于*2017*年计算机系统中的人为因素*CHI*会议论文集，2017年。

[76] Jonas Oppenlaender、Kristy Milland、Aku Visuri、Panos Ipeirotis 和 Simo Hosio。《付费众包平台上的创造力》。发表于*2020*年计算机系统中的人为因素*CHI*会议论文集，2020年。

[77] Kathryn Parsons、Agata McCormac、Malcolm Pattin- son、Marcus Butavicius 和 Cate Jerram。《探寻真相：一项关于用户对电子邮件行为反应的基于情境的实验》。发表于*2013*年*IFIP*国际信息安全会议论文集，2013年。

[78] Sarah Pearman、Shikun Aerin Zhang、Lujo Bauer、Nico- las Christin 和 Lorrie Faith Cranor。《为什么人们不能有效使用密码管理器》。发表于第*15*届可用隐私与安全研讨会论文集，2019年。

[79] Eyal Peer、Laura Brandimarte、Sonam Samat 和 Alessandro Acquisti。《超越土耳其机器人：用于行为研究众包的替代平台》。实验社会心理学杂志，70：153–163，2017年。

[80] 联合国开发计划署。《2019年人类发展报告》。https://hdr.undp.org/content/human-development-report-2019，（访问日期：2022年8月2日）。

[81] Lubna Razaq、Tallal Ahmad、Samia Ibtasam、Umer Ramzan 和 Shrirang Mare。“我们甚至向邻居借了钱”：通过受害者经历理解移动端诈骗。人机交互，5(CSCW)：1–30，2021年。

[82] Elissa M. Redmiles、Sean Kross 和 Michelle L Mazurek。我的调查结果能在多大程度上泛化？比较来自 MTurk、网络和电话样本的安全与隐私调查结果。载于第*40*届 *IEEE*安全与隐私研讨会论文集，2019。

[83] Elissa M. Redmiles、Noel Warford、Amritha Jayanti、Aravind Koneru、Sean Kross、Miraida Morales、Rock Stevens 和 Michelle L Mazurek。对网络上的安全与隐私建议进行全面质量评估。载于第*29*届 *USENIX*安全研讨会论文集，2020年。

[84] Benjamin Reinheimer、Lukas Aldag、Peter Mayer、Mat- tia Mossano、Reyhan Duezguen、Bettina Lofthouse、Tatiana Von Landesberger 和 Melanie Volkamer。关于网络钓鱼认知与教育随时间变化的调查：何时以及如何最好地提醒用户。载于第*16*届可用隐私与安全研讨会论文集，2020年。

[85] Simon Robinson、Jennifer Pearson、Thomas Reitmaier、Shashank Ahire 和 Matt Jones。让手机成为自我表达的工具：与新兴用户共同重新构想移动交互架构。载于*2018*年计算机系统中的人为因素*CHI*会议论文集，2018年。

[86] Nithya Sambasivan、Amna Batool、Nova Ahmed、Tara Matthews、Kurt Thomas、Laura Sanely Gaytán-Lugo、David Nemer、Elie Bursztein、Elizabeth Churchill 和 Sunny Consolvo。“无论我们走到哪里，他们都不让我们独处”：南亚的性别与数字虐待。载于*2019*年计算机系统中的人为因素*CHI*会议论文集，2019年。

[87] Nithya Sambasivan、Garen Checkley、Amna Batool、Nova Ahmed、David Nemer、Laura Sanely Gaytán- Lugo、Tara Matthews、Sunny Consolvo 和 Eliza- beth F. Churchill。“隐私与我无关，这是那些富裕女性的事”：南亚女性在手机上的表演性隐私实践。发表于第*14*届可用隐私与安全研讨会论文集，2018。

[88] Yukiko Sawaya、Mahmood Sharif、Nicolas Christin、Ayumu Kubota、Akihiro Nakarai 和 Akira Yamada。自信胜过知识：一项关于安全行为的跨文化研究。发表于*2017*年计算机系统人因*CHI*会议论文集，2017。

[89] Maxim Schessler、Eva Gerlitz、Maximilian Häring 和 Matthew Smith。Replication: 在德国复现智能手机安全与隐私领域的用户感知测量。发表于第六届欧洲可用安全研讨会论文集，2021年。

[90] Bingyu Shen、Lili Wei、Chengcheng Xiang、Yudong Wu、Mingyao Shen、Yuanyuan Zhou 和 Xinxin Jin。系统能否更好地解释权限？理解智能手机运行时权限模型下用户的错误认知。载于 第*30*届 *USENIX*安全研讨会论文集，2021年。[91] Yusuke Shinyama、Philippe Guglielmetti 和 Pieter Marsman。pdfminer.six。https://pdfminersix.readthedocs.io/en/latest/，（访问于2022年6月12日）。[92] Justin Smith、Lisa Nguyen Quang Do 和 Emerson Murphy-Hill。为什么 Johnny 无法修复漏洞：安全静态分析工具的可用性评估。载于 第*16*届可用隐私与安全研讨会论文集，2020年。[93] Ananta Soneji、Faris Bugra Kokulu、Carlos Rubio-Medrano、Tiffany Bao、Ruoyu Wang、Yan Shoshitaishvili 和 Adam Doupé。“存在缺陷，但正如民主制度一样，我们没有更好的系统”：专家对评估安全论文的同行评审流程的见解。载于 第*43*届*IEEE*安全与隐私研讨会论文集，2022年。[94] Peter Story、Daniel Smullen、Yaxing Yao、Alessandro Acquisti、Lorrie Faith Cranor、Norman Sadeh 和 Florian Schaub。网络隐私工具的认知、采用与误解。2021年。[95] Detmar Straub、Karen Loch、Roberto Evaristo、Elena Karahanna 和 Mark Srite。迈向基于理论的文化测量。《全球信息管理杂志》，10(1):13–23，2002年。[96] Monika Taddicken。社交网络中的“隐私悖论”：隐私顾虑、个体特征和感知到的社会相关性对不同形式自我披露的影响。《计算机媒介通信杂志》，19(2):248–273，2014年。[97] Mohammad Tahaei 和 Kami Vaniea。关于以开发者为中心的安全的调查。载于 第*4*届欧洲可用安全研讨会论文集，2019。

[98] Mohammad Tahaei 和 Kami Vaniea。招募具备编程技能的参与者：四个众包平台与计算机科学学生邮件列表的比较。载于*2022*年计算机系统中的人为因素*CHI*会议论文集，2022年。

[99] Joshua Tan、Lujo Bauer、Nicolas Christin 和 Lorrie Faith Cranor。结合最小强度、最小长度和黑名单要求，提出更强且更易用的密码的实用建议。载于 *2020*年 *ACM SIGSAC*计算机与通信安全会议论文集，2020年。

[100] Sabine Trepte、Leonard Reinecke、Nicole B. Ellison、Oliver Quiring、Mike Z. Yao 和 Marc Ziegele。关于隐私权衡的跨文化视角。社交媒体 + 社会，3(1)，2017年。[101] Blase Ur 和 Yang Wang。保护在线社交媒体中用户隐私的跨文化框架。载于第*22*届万维网国际会议论文集，2013年。[102] Christine Utz、Martin Degeling、Sascha Fahl、Florian Schaub 和 Thorsten Holz。（非）知情同意：实地研究《通用数据保护条例》同意通知。载于 *2019*年*ACM SIGSAC*计算机与通信安全会议论文集，2019年。[103] Amber Van Der Heijden 和 Luca Allodi。网络钓鱼攻击的认知分流。载于第*28*届*USENIX*安全研讨会论文集，2019年。[104] Melanie Volkamer、Andreas Gutmann、Karen Renaud、Paul Gerber 和 Peter Mayer。重复研究：对自动取款机及各种电子支付场景中现实世界个人识别码使用情况的跨国实地观察研究。载于第*14*届可用隐私与安全研讨会论文集，2018年。[105] Noel Warford、Tara Matthews、Kaitlyn Yang、Omer Akgul、Sunny Consolvo、Patrick Gage Kelley、Nathan Malkin、Michelle L Mazurek、Manya Sleeper 和 Kurt Thomas。SoK：统一高风险用户研究的框架。载于第*43*届*IEEE*安全与隐私研讨会论文集，2022年。[106] Rick Wash、Norbert Nthala 和 Emilee Rader。非专业用户在网络钓鱼检测中具备的知识与能力。载于第*17*届可用隐私与安全研讨会论文集，2021年。[107] Rick Wash 和 Emilee Rader。知识太多了吗？美国互联网用户的安全观念与防护行为。载于第*11*届可用隐私与安全研讨会论文集，2015年。

[108] Jason Watson、Heather Richter Lipford 和 Andrew Besmer。将用户偏好映射到隐私默认设置。*ACM* 人机交互汇刊，22(6):1–20，2015 年。

[109] Alma Whitten 和 J. D. Tygar。为什么 Johnny 无法加密：PGP 5.0 的可用性评估。载于 第 *8* 届 *USENIX*安全研讨会论文集，1999年。

[110] Yuxi Wu、W. Keith Edwards 和 Sauvik Das。SoK：社会网络安全。载于 第 *43* 届 *IEEE*安全与隐私研讨会论文集，2022年。

[111] Volker Wulf、Dave Randall、Konstantin Aal 和 Markus Rohde。个人即政治：伊朗伊斯兰共和国的互联网过滤与反向挪用。计算机支持的协同工作，31(2)：373–409，2022年。[112] Jeff Yan、Alan Blackwell、Ross Anderson 和 Alasdair Grant。密码可记忆性与安全：实证结果。*IEEE*安全与隐私，2(5)：25–31，2004年。[113] Yixin Zou、Kevin Roundy、Acar Tamersoy、Saurabh Shintre、Johann Roturier 和 Florian Schaub。考察安全、隐私和身份盗窃防护措施的采用与弃用。载于 *2020*年计算机系统中的人为因素*CHI*会议论文集，2020年。

附录

A 我们详细的筛选与编码规则

A.1 使用搜索查询进行筛选

在评审流程的第二阶段，我们使用第3.1节所述的搜索查询筛选论文。我们最初考虑使用数字图书馆的搜索功能，但由于发现 ACM数字图书馆的搜索功能无法准确运行，因此决定不采用该方法。具体而言，它遗漏了一些符合标准的论文。对于在其网站上发布 PDF文件的会议，我们以至少 10 秒的间隔下载文件。对于论文存储在数字图书馆中的会议，由于机器人访问禁令，我们手动下载 PDF文件。随后，我们使用 PDFminer.six 将 PDF数据转换为文本数据 [91]，并对每篇论文运行查询。我们初步确认了我们的搜索查询和脚本符合我们的标准。具体而言，我们对一个已完成全面评审的会议的所有接收论文运行了脚本，发现我们的脚本没有排除符合我们标准的论文。

表13：用于分析研究主题的简化编码手册。

研究主题	代表性描述和示例研究
总体	安全与隐私实践 [18]
访问控制和隐私偏好	数据收集场景的可接受性 [3] 权限设计 [90]
身份验证	密码生成和密码策略 [99] 辅助工具（例如密码管理器） [78]
漏洞/恶意软件/事件响应	安全软件开发实践 [69] 安全工具（例如，静态分析器） [92]
隐私侵害	亲密伴侣虐待（IPA） [65] 对其账户的未经授权的访问 [63]
社会工程	易受网络钓鱼攻击 [75] 网络钓鱼识别辅助工具 [12]
增强隐私技术	对隐私工具的（误）认知 [94] 隐私增强混淆技术 [60]

A.2 已审阅论文列表

表15 列出了我们在本研究中评审的 UPS论文。根据第3.1节所述的论文筛选流程，共有 715 篇论文接受了详细评审。

A.3 参与者所在国家的编码

图 3 展示了用于识别参与者所在国家的流程图。每项用户研究的参与者样本被划分为“已识别”“推断得出”或“未识别”。我们发现许多论文提供的描述含糊不清且信息不足。

A.4 研究主题的编码

为对 UPS 论文的研究主题进行分类，我们参考了Distler等人 工作中的研究主题分类 [32]。在该工作中，技术分类（例如“身份验证”）与侧重于用户感知和行为的分类（例如“安全感知、态度与行为”）被列在一起。后一种分类可应用于任何 UPS 论文。例如，分析用户对身份验证技术的安全感知的论文，可以归入任一类别。为消除分类歧义，我们仅依据技术对研究主题进行分类。

表13 展示了研究主题的简化编码手册及相应的代表性论文。

- “总体”包括调查用户对广泛的安全与隐私相关技术的感知、态度和行为，但不专注于特定技术的研究。
- “访问控制与隐私偏好”包括调查用户对其数据的隐私顾虑、偏好和实践，并评估隐私控制工具可用性的研究。
- “身份验证”包括研究身份验证技术及其支持工具的安全性和可用性的研究。
- “漏洞/恶意软件/事件响应”包括研究漏洞和事件相关响应技能与实践，以及评估支持工具可用性的研究。
- “隐私侵害”包括调查用户隐私所面临威胁的研究，例如幸存者的防御实践与担忧，以及施害者的手段。
- “社会工程”包括研究用户易受社会工程攻击的程度和防御实践的研究，也包括研究对策（例如，警告）有效性的研究。
- “隐私增强技术”包括研究用户对隐私增强技术（例如虚拟专用网络和端到端加密）的（错误）理解和使用情况。
- “其他”包括专注于上述所列技术或威胁以外的任何研究，例如对抗性攻击（例如向个人助理中插入恶意命令）。

B 使用 AND 运算符的 WEIRD

在第4.1节、4.2节和4.3节中，我们已经表明，使用 OR 逻辑运算符时，大多数 UPS 参与者样本来自 WEIRD国家。我们还关注参与者样本来自完全 WEIRD国家的比例，即使用 AND 作为逻辑运算符的情况。与 Linxen研究类似，我们将 UPS论文曾经研究过一次或多次的国家在 E、I、R 和 D 四个维度分布的中位数设为截断值。需要注意的是，这项分析展示的是 UPS论文所研究国家中相对完全 WEIRD的国家，而非全球所有国家中完全 WEIRD的国家。在 791 个参与者样本中，我们发现，75.22% 是在完全 WEIRD国家招募的，3.67% 是在西方但非“EIRD”的国家招募的，2.53% 是在非西方但属于“EIRD”的国家（例如以色列和日本）招募的，其余 18.58% 则是在完全非 WEIRD国家（例如印度和孟加拉国）招募的。

C 霍夫斯泰德的文化维度

我们使用霍夫斯泰德文化维度框架进行了补充分析 [46, 50]。该框架用于理解文化差异，包含六个文化维度，如表14所示。尽管该框架无法解释所有文化差异，但我们认为这些维度与UPS研究相关。例如，权力距离较高的国家在政府参与信息隐私监管方面表现出显著更高的程度 [25, 68]。关于社交媒体上的信息披露，Trepte等人 [100] 重点关注了先前研究中相互矛盾的研究结果：（1）来自个人主义文化背景的人

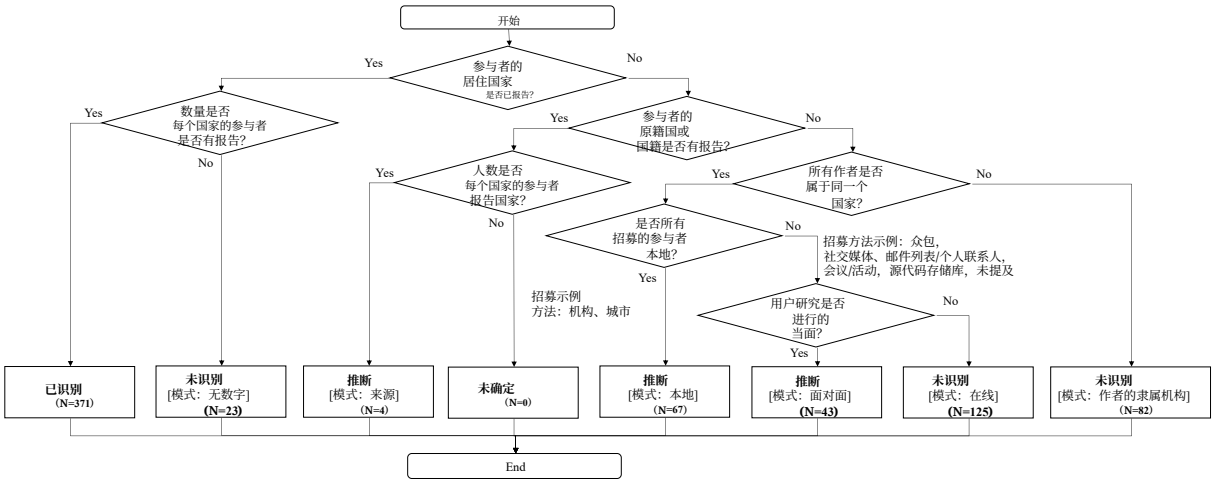

图 3：识别或推断参与者所在国家的流程图。

文化更有可能规避隐私风险，并且（2）来自集体主义文化的人更有可能规避这些风险。他们的研究结果支持了后者的发现。关于网络钓鱼，Butavicius 等人证明，来自个人主义文化的用户更不容易受到网络钓鱼邮件的影响 [20]。

表 14：Ψs 与文化维度的相关性。

指标	r
权力距离	-.44***
个人主义（相对于集体主义）	.43***
男性气质（相对于女性气质）	-.09
不确定性规避	-.08
长期导向（相较于短期导向）	.13
放纵（相对于克制）	.09

我们收集了每个国家在六个维度上的得分 [50]，并计算了各国 $\Psi_{\text{参与者样本}}$ 与文化维度各项指标之间的相关性。我们发现，$\Psi_{\text{参与者样本}}$ 与权力距离呈负相关（r =-.44，p <.001），与个人主义呈正相关（r =.43，p <.001）。也就是说，UPS论文中的大多数参与者样本来自权力分配较为平等的个人主义文化。结合先前研究的发现和我们的分析，我们强调，大多数UPS论文所研究的人群可能主要来自这样一些国家：这些国家的居民更有可能在社交媒体上披露自己的信息，同时也较不容易遭受网络钓鱼攻击。

表15：已审阅论文列表（N =715）。

会议	Year	标题
S&P	2017	SmarPer：面向移动设备的上下文感知与自动运行时权限管理
S&P	2017	Cloak and Dagger：从两个权限到对用户界面反馈循环的完全控制
S&P	2017	XHOUND：量化浏览器扩展的可指纹识别性
S&P	2017	密码学 API 的可用性比较
S&P	2017	工业机器人控制器的实验性安全分析
S&P	2017	密码重置中间人攻击
S&P	2017	SysPal：适用于安卓的系统引导图案锁
S&P	2017	利用手部几何特征和行为信息进行多点触控身份验证
S&P	2017	动态授予权限的可行性：使移动隐私与用户偏好保持一致
S&P	2017	无瑕沙箱：利用磨损痕迹逃避恶意软件分析系统
S&P	2017	采用安全通信工具的障碍
S&P	2018	两个研究的故事：YubiKey 可用性的最佳与最差表现
S&P	2018	美国难民的计算机安全与隐私
S&P	2018	你能感受到我听到的吗？使用不同传感器类型实现自主物联网设备配对
S&P	2018	EyeTell：基于眼动的视频辅助触摸屏击键推断
S&P	2018	黑客与测试人员：软件漏洞发现流程比较
S&P	2018	关于增强大型人道主义组织的数字免疫力
S&P	2018	Facebook 基于个人身份信息的定向投放所带来的隐私风险：审查数据经纪商的广告界面
S&P	2018	迈向多用户增强现实的安全与隐私：以终端用户为基础
S&P	2018	当健身追踪器背叛你：量化生物特征在不同情境下的可预测性
S&P	2019	揭开移动应用中隐藏的隐私设置
S&P	2019	Tap 'n Ghost：针对智能手机触摸屏的新型攻击技术汇编
S&P	2019	“我是否应该担心？”账户安全事件响应的跨文化考察
S&P	2019	“如果 HTTPS 是安全的，“我不需要双重身份验证”——终端用户和管理员的 HTTPS 心智模型
S&P	2019	危险技能：理解并缓解虚拟个人助理上语音控制的第三方功能所带来的安全风险
S&P	2019	助手系统 我的研究结果能多大程度上泛化？比较来自 MTurk、网络和电话样本的安全与隐私调查结果
S&P	2020	专家问答：物联网隐私与安全标签上应包含哪些内容?
S&P	2020	自动检测照片中的旁观者，以降低隐私风险
S&P	2020	选民能否识别对选票标记设备的恶意操纵?
S&P	2020	智能手机上的手势认证：手势密码选择策略评估
S&P	2020	影响社交媒体上的照片分享决策：一个矛盾性发现案例
S&P	2020	FIDO2 是用户身份验证的弑王者吗？FIDO2 无密码认证的可用性比较研究
S&P	2020	安全更新标签：为物联网消费产品的安全补丁建立经济激励
S&P	2020	SPIDER：加速相关软件仓库中的补丁传播
S&P	2020	这个个人识别码很容易被猜中：分析智能手机解锁个人识别码的安全性
S&P	2020	迈向智能家居的自然视角：实用的安全与安全性分析
S&P	2020	迈向有效的差分隐私沟通，以助力用户的数据共享决策与理解
S&P	2020	WaveSpy：通过毫米波感知实施远程及穿墙屏幕攻击
S&P	2021	苏丹革命期间政治活动人士对防御性技术的使用
S&P	2021	HackEd：对在线漏洞发现练习的教学法分析
S&P	2021	听见“邪恶”，看见“Kenansville”：针对语音识别和语音识别的高效且可迁移的黑盒攻击系统
S&P	2021	摄像头和激光雷达均无法探测：物理世界环境下自动驾驶多传感器融合感知的安全性攻击
S&P	2021	蓝牙配对中的方法混淆攻击
S&P	2021	哪些隐私与安全属性最影响消费者对风险的感知以及购买物联网设备的意愿?
S&P	2021	谁是真正的鲍勃？针对说话人识别系统的对抗性攻击
SEC	2017	“我完全不知道自己在做什么”——论部署 HTTPS 的可用性
SEC	2017	当最薄弱的链接变得牢不可破：巴拿马文件事件中的安全协作
SEC	2017	AWare：通过操作绑定防止滥用隐私敏感传感器
SEC	2017	探索用户对在线定向广告中歧视现象的认知
SEC	2017	扩展程序崩溃：浏览器扩展程序资源控制政策的安全分析
SEC	2017	6thSense：面向智能设备的基于情境感知传感器的攻击检测器
SEC	2017	SmartAuth：面向物联网的以用户为中心的授权
SEC	2017	跨设备跟踪的隐私分析
SEC	2018	密码遗忘：生态学理论与数据
SEC	2018	Polisis：利用深度学习自动分析与呈现隐私政策
SEC	2018	重新思考家庭物联网（IoT）的访问控制与身份验证
SEC	2018	电子邮件欺骗攻击的端到端测量
SEC	2018	管理是否胜过记忆？探究管理器对密码强度与重复使用的影响
SEC	2018	理解众包报告的安全漏洞的可复现性
SEC	2018	纽约之战：企业级应用数字威胁建模案例研究
SEC	2018	Tor 用户如何与洋葱服务互动?
SEC	2018	CommanderSong：实用对抗性语音识别的系统化方法
SEC	2018	你们的全球定位系统都归我们所有：迈向对道路导航系统的隐蔽操纵
SEC	2018	大型学术机构遭受加密勒索软件攻击后的影响
SEC	2019	评估隐私法规的情境完整性：家长的物联网玩具隐私规范与儿童在线隐私保护法之比较
SEC	2019	受害者服务提供者与人口贩运幸存者互动中的计算机安全与隐私
SEC	2019	Stack Overflow 被认为很有帮助！通过深度学习安全助推来强化密码学
SEC	2019	面向亲密伴侣暴力受害者的临床计算机安全
SEC	2019	通过 Apple Wireless Direct 攻击十亿个开放接口：针对 iOS 和 macOS 的中间人攻击、拒绝服务攻击与跟踪攻击——Eve 和 Mallory 的视角 Link
SEC	2019	Web 身份危机：了解网站身份指示器的有效性
SEC	2019	理解与改进多用户智能家居中的安全与隐私：一项设计探索与家庭用户研究
SEC	2020	“我看不见的东西，分享起来让我感到不安”：视障人士使用基于摄像头的辅助应用时的隐私顾虑
SEC	2020	人类可辨识的可视密钥指纹

会议	Year	标题
SEC	2020	另一种 TI？商业威胁情报的附加价值
SEC	2020	Chaperone：面向智能手机的实时锁定与损失防范
SEC	2020	Devil's Whisper：针对商业黑盒语音识别设备的物理对抗攻击通用方法
SEC	2020	广告拦截器对产品搜索与购买行为的影响：一项实验室实验
SEC	2020	黑客攻击的工业时代
SEC	2020	对抗性预处理：理解并防范机器学习中的图像缩放攻击
SEC	2020	网络安全与隐私建议的全面质量评估
SEC	2020	“我非常尊重长辈”：了解南非移动用户对隐私的感知及其当前在 Facebook 和 WhatsApp
SEC	2020	视而不见：利用虚假透明度进行权限网络钓鱼
SEC	2020	逆向工程师工作流程的观察性研究
SEC	2020	Twitter 知道些什么：通过用户自己的 Twitter 帖子，刻画广告定向实践、用户认知与广告解释 Data
SEC	2020	从需求到行动，打造安全应用？需求与开发者实践对应用安全的影响
SEC	2020	活体检测并不足够：利用行为生物识别增强指纹认证，以抵御傀儡攻击
SEC	2021	PhishPrint：通过预先画像规避钓鱼检测爬虫
SEC	2021	评估工作流内消息对改善端到端加密心智模型的作用
SEC	2021	大规模城市抗议中的集体信息安全：香港案例
SEC	2021	低成本脑电波认证：关于用户接受度的新技术与见解
SEC	2021	关于用户对 Android 权限的行为、预期与参与度的大规模研究
SEC	2021	mID：通过莫尔条纹追踪屏幕照片
SEC	2021	“为什么不会有人把民主视为目标？”：参与美国政治宣传活动
SEC	2021	充电器冲浪：利用电力线侧信道实现智能手机信息泄露
SEC	2021	Dompteur：驯服音频对抗样本
SEC	2021	解释胜过情境：时机与理由对用户运行时权限决策的影响
SEC	2021	隐私仪表板对终端用户有益吗？评估用户对 Google“我的活动”的认知与反应
SEC	2021	考察基于诱饵的心理网络欺骗的有效性
SEC	2021	HAWatcher：应用化智能家居的语义感知异常检测
SEC	2021	视觉推理验证码安全性研究
SEC	2021	情绪的影响 ，位置 ，信任, 以及他人在场对基于视频的社交认证的影响
SEC	2021	“是公司、政府、你和我”：用户对智能家居隐私与安全责任的认知
SEC	2021	评估针对基于国际化域名的网络钓鱼的浏览器级防御
SEC	2021	关于中小企业信息安全及其遭受攻击的大规模访谈研究
SEC	2021	调整安全警告以应对在线虚假信息
SEC	2021	帮助用户自动查找和管理云存储中的敏感且可舍弃文件
SEC	2021	PriSEC：隐私设置执行控制器
SEC	2021	一种利用蜂窝网络载波聚合的隐蔽位置识别攻击
SEC	2021	“这些数据应该存储在加密服务器上”：消除用户对 FIDO2 生物特征 WebAuthn 的误解
SEC	2021	AdCube：WebVR 广告欺诈与第三方广告的实用隔离
SEC	2021	Kaleido：眼动追踪系统的实时隐私控制
SEC	2021	网络上的有效通知活动：信任、框架效应与支持
SEC	2021	“我现在有点生气”：个人对影响自身的数据泄露的认知、感知与应对
SEC	2021	“要管理这么多部手机，真让人压力很大”：调查性工作者在线上的安全目标、风险与实践
SEC	2021	先共享，后询问（还是永不询问？）：研究 Android 应用违反《通用数据保护条例》明确同意要求的情况
SEC	2021	硬件安全令牌真实性检查的可用性
SEC	2021	声学来助力：重新审视物理密钥推断攻击
SEC	2021	老年人为什么（不）使用密码管理器
SEC	2021	脏污道路也能发动攻击：物理世界攻击下基于深度学习的自动车道居中安全性
SEC	2021	系统能否更好地解释权限？理解智能手机运行时权限模型下用户的误解
SEC	2021	鱼与熊掌兼得：对让步滥用即服务的分析
SEC	2021	“密码让我安全”——了解儿童对密码的看法
SEC	2021	FIDO 能否消除实时网络钓鱼？针对 FIDO协议的社会工程降级攻击
SEC	2021	发送敏感文件的策略与感知风险
SEC	2021	从首席信息安全官的视角看小型企业面临的安全障碍与动机
SEC	2021	计算机安全客户支持在帮助亲密伴侣暴力幸存者方面的作用
CCS	2017	仅凭听到你的声音还不够：用于语音认证的基于发音手势的活体检测
CCS	2017	VibWrite：通过物理振动实现无处不在的表面上的手指输入认证
CCS	2017	让我们进一步仔细观察：在自然环境中观察密码
CCS	2017	防患于未然：支持 Android 开发者编写安全代码
CCS	2017	TypTop 系统：个性化容错密码校验
CCS	2017	CCCP：隐藏字幕加密手机，抵御中间人攻击、人为错误和点击通过
CCS	2017	量化法律风险对第三方漏洞研究的压力
CCS	2017	随时向我通报：安卓第三方库可更新性的实证研究
CCS	2017	为什么开发者会在密码存储上出错？一项定性可用性研究
CCS	2018	替朋友提问：评估安全用户研究中的响应偏差
CCS	2018	迈向易用的校验和：为大众自动化网络下载的完整性验证
CCS	2018	又一个文本验证码求解器：一种基于生成对抗网络的方法
CCS	2018	无需训练障碍：快速实施与训练无关的攻击以推断你的打字内容
CCS	2018	通过隐式学习强化系统分配的密码短语
CCS	2018	“那个网站拿我的 Facebook 密码做了什么？”密码重复使用通知的设计
CCS	2018	欺诈去匿名化：为了乐趣与利益
CCS	2018	PatternListener：利用声学信号破解安卓图案锁
CCS	2018	根据用户行为预测即将遭遇恶意内容暴露
CCS	2018	探究系统运营人员对安全配置错误的看法
CCS	2018	剥开洋葱的用户体验层：考察 Tor 浏览器的自然使用情况
CCS	2019	Google Play 中欺诈性应用程序推广的艺术与技巧
CCS	2019	“我看不出自己为什么会想用它”：分析热门智能手机密码管理器的可用性
CCS	2019	超越社交媒体上一劳永逸式的隐私设置

会议	Year	标题
CCS	2019	（非）知情同意：研究《通用数据保护条例》同意通知
CCS	2019	28 次眨眼之后：应对眼动生物特征识别的实际挑战
CCS	2019	匹配与不匹配的安全运营中心：关于安全运营中心问题的定性研究
CCS	2019	Velody：用于增强用户身份验证韧性的非线性振动质询-响应
CCS	2019	田野里的捕手：一种基于声纹的文本无关说话人验证欺骗检测方法
CCS	2019	你看起来是什么人，就是什么人：TLS 证书中域名冒充的纵向研究
CCS	2019	哦，你去过这些地方！用户对第三方网络跟踪与推断的长期透明度的反应
CCS	2019	Let's Encrypt 和 Certbot 的可用性评估：正确实现可用安全
CCS	2020	依赖项管理及其安全影响的定性研究
CCS	2020	T2Pair：异构物联网设备的安全且易用配对
CCS	2020	利用环境射频噪声进行可穿戴设备配对
CCS	2020	兼顾最低强度、最小长度和黑名单的实用建议：打造更强且更易用的密码需求
CCS	2020	危险技能获认证：衡量语音个人助理平台中技能认证的可信度
CCS	2020	隐私增强技术的使用模式
CCS	2020	内核利用中弹性对象的系统性研究
CCS	2020	Mnemosyne：一种有效且高效的事后水坑攻击调查系统
CCS	2021	Periscope：一种利用人体耦合电磁辐射的击键推断攻击
CCS	2021	使用振动实现智能手表上的易用用户身份验证
CCS	2021	谁在控制？论割裂的物联网设备管理渠道所带来的安全风险
CCS	2021	“喂，是我”：现实世界中的基于深度学习的语音合成攻击
CCS	2021	深入了解恶意软件分析实践
CCS	2021	谷歌搜索对软件安全的影响：通过内容重新排序实施不显眼的安全干预
CCS	2021	十二位愤怒的开发者：关于开发者在 CSP 方面所遇困境的定性研究
CCS	2021	WristPrint：探究从腕戴式加速度计数据中重新识别用户的风险
CCS	2021	“我需要更好的描述”：对用户对于差分隐私的预期进行调查
NDSS	2017	通过高效浏览快照实现对用户攻击的重构
NDSS	2017	心碎：如何攻击心电图生物识别系统
NDSS	2017	迈向基于隐式视觉记忆的身份验证
NDSS	2017	KEH-Gait：迈向基于动能收集的移动医疗用户身份验证系统
NDSS	2017	五次尝试破解安卓图案锁
NDSS	2018	你没听见我吗？——迈向更成功的 Web 漏洞通知
NDSS	2018	rtCaptcha：一种基于实时验证码的活体检测系统
NDSS	2018	BC：通过内置摄像头启用智能手机身份验证
NDSS	2018	轻触电极即可完成设备配对
NDSS	2018	面部闪光：一种基于光反射的安全活体检测协议
NDSS	2018	多主体互依赖数据的共识式隐私保护共享
NDSS	2018	JavaScript Zero：真正的 JavaScript，零侧信道攻击
NDSS	2019	清理邪恶事物构成的互联网：ISP 和消费者移除 Mirai 的真实世界证据
NDSS	2019	TEXTBUGGER：针对真实世界应用程序生成对抗性文本
NDSS	2019	数量与质量：使用广告偏好管理器评估用户兴趣档案
NDSS	2019	通过保留缩略图的加密，在图像隐私与可用性之间取得平衡
NDSS	2019	通过心理声学隐藏对自动语音识别系统发起对抗性攻击
NDSS	2019	语音安全（与不安全）的关键：关于说话者身份合法性检测的脑部研究
NDSS	2019	语音识别之后的生活：针对语音助手应用的语义误解模糊测试
NDSS	2020	来自驾驶舱的视角：探索飞行员对航空电子系统遭受攻击的反应
NDSS	2020	OcuLock：探索人类视觉系统在虚拟现实头戴式显示器身份验证中的应用
NDSS	2020	你会接听吗？衡量用户对反自动骚扰电话应用指示器的响应
NDSS	2021	聚焦按键：利用视频通话实施击键推断攻击
NDSS	2021	你的手机就是我的代理：移动代理网络的检测与理解
NDSS	2021	现代移动设备上的短信一次性密码消息无法抵御本地攻击者
NDSS	2021	PFIREWALL：面向智能家居隐私保护的语义感知型可定制数据流控制
NDSS	2021	PrivacyFlash Pro：自动生成移动应用的隐私政策
NDSS	2021	迈向理解和检测真实世界图像中的网络欺凌
PETS	2017	授权前请三思：利用眼动追踪强化用户对应用程序权限的关注
PETS	2017	跨文化隐私预测
PETS	2017	针对政府反对者的社会工程攻击：目标视角
PETS	2017	Tor 启动器的可用性评估
PETS	2017	为什么隐私几乎被遗忘
PETS	2017	允许还是不允许，这是可用性问题：通过众包研究移动应用的隐私权限设置
PETS	2018	你所做的每一个动作：探索智能手机运动传感器指纹识别的实际问题及对策
PETS	2018	识别并模仿程序员风格：程序作者归属判定中的对手
PETS	2018	破解 ShadowCrypt：探索互联网浏览器中安全输入/输出系统的局限性
PETS	2018	触摸，你就会落入陷阱：量化触摸手势用于跟踪的独特性
PETS	2018	削弱航空通信寻址与报告系统（ACARS）中的隐私保护
PETS	2019	系统化基因组隐私研究：隐私增强技术视角
PETS	2019	（共同）位置共享博弈
PETS	2019	利用动态应用沙箱缓解移动设备上的位置隐私攻击
PETS	2019	跳过，跳过，再跳过，接受！！！：智能手机制造商提供的默认功能的可用性与用户隐私研究
PETS	2019	AccessiLeaks：调查 Android 无障碍服务暴露的隐私泄露
PETS	2019	探究人对隐私风险的感知
PETS	2019	#DontTweetThis：为社交网络中的私人信息评分
PETS	2019	“如果……会怎样？”预测个体用户的智能家居隐私偏好及其变化
PETS	2019	智能音箱用户的隐私态度
PETS	2020	《通用数据保护条例》之后的隐私政策格局
PETS	2020	采用和弃用虚拟专用网络作为隐私增强技术的情感与实践考量
PETS	2020	没有 PETS 的宠物：宠物主人低估宠物可穿戴设备中的隐私顾虑
PETS	2020	两全其美：缓解捕获移动应用隐私偏好时准确性与用户负担之间的权衡
PETS	2020	保护隐私的支付拆分

会议	Year	标题
PETS	2020	解释隐私增强技术的技术使用行为：以 Tor 和 JonDonym 为例
PETS	2020	SPy：汽车转向揭示你的行程路线！
PETS	2020	只有在被唤醒时才聆听：将人际通信线索作为智能音箱的隐私控制手段
PETS	2020	一览隐私：以用户为中心的可快速浏览的数据暴露可视化设计
PETS	2020	爱彼迎中的智能设备：兼顾房客与房东的隐私与安全
PETS	2020	多重目的，多重问题：GDPR 实施后关于同意对话框的用户研究
PETS	2020	浏览器指纹识别的长期观察：用户可追踪性与观点
PETS	2020	价格是否公道：比较免费和付费应用中的隐私保护
PETS	2020	未走之路：重新思考通过 Tor 进行语音通话的可行性
PETS	2020	通过组合式释义实现有效的写作风格迁移
PETS	2021	通过代码挖掘和机器学习揭示真实环境中的网络指纹识别
PETS	2021	隐私（不）感知物联网应用的实时分析
PETS	2021	“提醒他们”还是“直接屏蔽他们”？：探究老年人与劳动年龄成年人的隐私顾虑
PETS	2021	隐私政策中数据实践的自动提取与呈现
PETS	2021	利用个性化噪声防御基于麦克风的攻击
PETS	2021	互联网用户信息隐私顾虑量表（IUIPC）的效度与信度
PETS	2021	“你知道这台摄像机在追踪你的情绪吗？”：理解视频分析时代的隐私期望与偏好
PETS	2021	Face-Off：对抗性人脸模糊处理
PETS	2021	探索德国办公室职员对信息自决权的心智模型
PETS	2021	有动机者能够加密（即使用 PGP 也一样）
PETS	2021	隐私的定义：用户如何解读隐私政策中的技术术语
PETS	2021	网络隐私工具的认知、采用及误解
PETS	2021	隐私在数字化中的作用——分析德国农民的观点
PETS	2021	从自我披露的视角看数字不平等
PETS	2021	ZKSENSE：一种适用于移动设备、无摩擦且保护隐私的人类证明机制
PETS	2021	“我必须评估他们的异议”：智能家居设备所有者与偶然用户之间的隐私张力
PETS	2021	“我们三兄弟一直以来都对彼此了如指掌”：关于数字设备共享与在线账户
PETS	2021	管理浏览器中可能具有侵扰性的做法：以用户为中心的视角
CHI	2017	保持冷静！了解针对基于移动设备的用户身份验证的热攻击
CHI	2017	变色龙设备：探究通过主动伪装实现更安全、更隐蔽的移动交互
CHI	2017	高成本与小收益：一项关于用户如何体验操作系统升级的实地研究
CHI	2017	知己知彼，百战不殆：揭示智能手机应用的数据共享实践
CHI	2017	父母和儿童对于父母在社交媒体上分享儿童相关信息的偏好
CHI	2017	“天空中的蜘蛛”：用户对无人机、隐私和安全的认知
CHI	2017	了解现实环境中的偷窥屏幕：来自用户和旁观者的故事
CHI	2017	社交媒体中的照片隐私冲突：一项大规模实证研究
CHI	2017	探索差分隐私：人们何时信任随机响应技术?
CHI	2017	安卓上的用户交互与权限使用
CHI	2017	独角兽能帮助用户比较加密密钥指纹吗?
CHI	2017	会倾听的玩具：一项关于父母、儿童和联网玩具的研究
CHI	2017	我太忙了，没空重置我的 LinkedIn 密码：论密码重置邮件的有效性
CHI	2017	剖析面向老年人与青年人的鱼叉式网络钓鱼邮件：影响力武器与生活领域在预测中的交互作用易受网络钓鱼攻击的程度
CHI	2017	设计社交网络系统以支持成功衰老时的隐私考量
CHI	2017	通过 Mobile Roadwatch 促进道路上的普遍性社区警务
CHI	2017	幸存者的故事：应对亲密伴侣虐待时的隐私与安全实践
CHI	2017	随着时间推移，我们对警告习惯化的发生过程究竟了解多少？关于习惯化与多态警告
CHI	2017	Facebook 上社交内部攻击的特征分析
CHI	2017	FDVT：面向脸书用户的数据估值工具
CHI	2017	无人机的隐私机制：无人机操控者与旁观者的看法
CHI	2017	人能准确地自我报告安全行为吗？自我报告与行为测量之间的一致性
CHI	2017	我的消息被读了吗？：Facebook Messenger 上的隐私与信号传递
CHI	2017	自信胜过知识：安全行为的跨文化研究
CHI	2017	全球南方的隐私、安全与监控：孟加拉国生物识别移动 SIM 卡注册研究
CHI	2017	利用个人数据驱动个性化电子节目指南所面临的挑战
CHI	2017	Thumprint：通过共享秘密敲击实现具备社会包容性的本地群组身份验证
CHI	2017	在公共空间自由飞行：无人机操控者的隐私认知与实践
CHI	2017	数据驱动型密码强度计的设计与评估
CHI	2018	突发！安全与隐私新闻的类型学及其传播方式
CHI	2018	遮挡照片中的场景元素以增强隐私的观看体验
CHI	2018	隐私谎言：了解人们如何、何时以及为何在多种在线情境中撒谎以保护隐私
CHI	2018	利害攸关之处：刻画新兴技术的风险认知
CHI	2018	图形密码设置过程中人类认知与视觉行为对密码强度的影响
CHI	2018	低调行事？无证移民群体中的技术、风险与隐私
CHI	2018	理解家庭视角下家庭公民数据的存储、共享与处理
CHI	2018	评估针对智能手机 PIN 码偷窥屏幕攻击的攻击与防御策略
CHI	2018	我究竟投了什么？论可验证电子投票方案的可用性
CHI	2018	作为计划行为的网络摄像头遮挡
CHI	2018	控制还是安全？考察家长在青少年移动设备上使用技术监控应用
CHI	2018	通过基于漫画的政策提升用户注意力
CHI	2018	ResearchIME：用于在真实环境中研究自由打字行为的移动键盘应用程序
CHI	2018	应用程序开发期间的安全：一位应用程序安全专家的视角
CHI	2018	将隐私决策置于情境中，以实现更好的预测（和保护）
CHI	2018	从扫描大脑到读取思想：与工程师探讨脑机接口
CHI	2018	通过视觉屏蔽，在交互式记录链接中平衡隐私与信息披露
CHI	2018	X-Ray Refine：支持探索和优化智能手机应用造成的信息暴露
CHI	2018	让手机成为自我表达的舞台：与新兴用户共同重新构想移动交互架构

会议	Year	标题
CHI	2018	剖析在线定向与个性化背后数据驱动推断的感知
CHI	2018	一项关于用户在实际场景中对浏览器警告反应的经验抽样研究
CHI	2018	“此应用程序希望使用您的当前位置，以便为您提供更好的服务”：用户同意与系统透明度在个性化移动服务中的重要性
CHI	2018	遗忘却未消失：识别云存储中纵向数据管理的需求
CHI	2018	利用语义转换研究密码习惯及其成因
CHI	2018	“跟踪者的天堂”：亲密伴侣施虐者如何利用技术
CHI	2019	“无论我们走到哪里，他们都不让我们安宁”：南亚的性别与数字虐待
CHI	2019	情境因素对 Snapchat 公开共享的影响
CHI	2019	过渡性无家可归者收容所的艰难时期：探讨经济不安全对数字安全与隐私的影响
CHI	2019	我甚至都不用打扰他们！利用社交媒体自动化安全消息传递中的身份验证流程
CHI	2019	“我编了个傻乎乎的名字”：理解儿童对在线隐私风险的认知
CHI	2019	What.Hack：通过角色扮演式网络钓鱼模拟游戏开展引人入胜的反网络钓鱼培训
CHI	2019	“如果你愿意，我可以存储加密后的密码。”——一项针对自由职业开发者的密码存储实地研究
CHI	2019	“几乎是必备项”：在生物识别采用中平衡可用性诉求与安全顾虑
CHI	2019	迈向理解年龄与智能手机身份验证之间的关联
CHI	2019	“每个人都有一些私人内容”：为孟加拉国共享手机使用设计数字隐私支持方案
CHI	2019	守护我的城堡：智能家居隐私机制的协同设计研究
CHI	2019	嘿，谷歌，我可以私下问你一些事情吗？模态和设备对获取敏感健康信息的影响来自语音助手
CHI	2019	风险与限制：在为寄养青少年营造正常感与保障他们的在线安全之间的矛盾
CHI	2019	谁在控制？：多用户智能家居中的 Interactions
CHI	2019	亚马逊土耳其机器人上的隐私、权力与隐形劳动
CHI	2019	“从一开始就考虑安全”：对软件开发人员的调查
CHI	2019	小学数字技术使用中的隐私与安全考量
CHI	2019	关系不止是字节：重新思考智能服务为人与事物带来的益处
CHI	2019	HTTPS 部署的可用性
CHI	2019	轻度认知障碍老年人在线安全中的上行与下行风险
CHI	2019	“如果重要，就会成为头条”：老年人的网络安全信息搜寻
CHI	2019	隐私能否令人满意？利用美学变换提升隐私增强照片的观看者满意度
CHI	2019	安全管理者也不是敌人。
CHI	2019	将警告放在链接所在之处：改进并评估电子邮件网络钓鱼警告
CHI	2019	了解信息表征对信息共享意愿的影响
CHI	2019	探索隐私与安全如何影响物联网设备的购买行为
CHI	2019	机器启发式：当我们比信任人类更信任计算机来保管个人信息
CHI	2019	漏洞与归责：理解智能手机遭未经授权访问
CHI	2019	承诺就是承诺：承诺装置对计算机安全意图的影响
CHI	2019	安全——看得见，却未察觉？展示安全机制如何影响用户体验与感知安全
CHI	2019	开放协作中的隐私、匿名性与感知风险：服务提供商研究
CHI	2019	Passquerade：使用图形滤镜改进移动设备上文本密码的错误纠正与密码掩码
CHI	2019	男同性恋者和双性恋者使用的性社交应用中，明确的艾滋病病毒状态披露字段的信号挪用
CHI	2020	倾听开发者的声音！一项针对密码学 API 安全警告的参与式设计研究
CHI	2020	评估敏感信息披露中的“倾向于不透露”选项
CHI	2020	这个 URL 的目标地址是什么？对用户 URL 阅读行为的实证评估
CHI	2020	3D-Auth：使用个性化 3D 打印物品进行双因素认证
CHI	2020	信息过载：质疑后数字社会中的安全
CHI	2020	用户对在线状态指标的体验
CHI	2020	家庭之外的智能家居：社区型访问控制的必要性
CHI	2020	为互联家庭中的隐私赋能工具设计提供依据
CHI	2020	使用统一资源定位符衡量身份混淆
CHI	2020	可穿戴麦克风干扰
CHI	2020	家庭人际空间中个人代理的社会边界
CHI	2020	《通用数据保护条例》之后的暗黑模式：抓取同意弹窗并展示其影响
CHI	2020	跨性别群体中的隐私与行动主义
CHI	2020	弱化较早社交媒体内容的呈现对模拟招聘决策的影响
CHI	2020	评估智能手机用户的信息安全意识
CHI	2020	为物联网个性化隐私助手的设计提供参考
CHI	2020	脱离情境使用数据以实现超个性化广告：众包工作者的隐私认知及其披露私人信息的决策信息
CHI	2020	评估隐私浏览模式的终端用户体验
CHI	2020	迈向照片内容敏感度与分享偏好的分类体系
CHI	2020	“简直像寻宝”：网站退出与数据删除选项的可用性
CHI	2020	亚马逊还是我兄弟：共享智能音箱用户如何看待并应对隐私风险
CHI	2020	删除历史记录能让 Alexa 更值得信任吗？隐私与内容定制对智能设备用户体验的影响演讲者
CHI	2020	信任与隐私：在点对点汽车共享中使用联网汽车数据
CHI	2020	探究安全、隐私和身份盗窃防护措施的采用与弃用
CHI	2020	隐私沟通中的情境真的重要吗？——一项关于消费者顾虑与偏好的调查
CHI	2020	我眼观六路、耳听八方：探索物联网情境下提升隐私意识的有效定位器
CHI	2020	“我们彼此监督、各负其责”：深入剖析社交群体如何共同应对网络安全与隐私问题
CHI	2020	“青柠色”、“打开的锁”和“已屏蔽”：儿童对网络安全警告中颜色、符号和文字的认知
CHI	2020	终止在线账户共享的代价
CHI	2020	了解健身追踪器用户的安全与隐私知识、态度和行为
CHI	2020	剑桥分析事件之后的所有权、隐私与控制：态度与认知之间的关系
CHI	2020	机器人电话：STIRRED AND SHAKEN！——来电显示对信任和接听率的影响研究
CHI	2020	应对匿名滥用行为：衡量技术机制对用户报告行为的影响
CHI	2020	信任圈：面向家庭的移动网络安全新方法
CHI	2020	构建并验证安全软件开发自我效能量表
CHI	2020	通过数字化赋能公民：格陵兰女性案例

会议	Year	标题
CHI	2020	提升瑞士互联网投票界面的可用性和用户体验
CHI	2020	如何与计算机科学专业学生开展安全开发者研究：与计算机科学专业学生、自由职业者开展密码存储研究，以及公司开发人员
CHI	2020	“我希望他们是一家有道德的公司，不会做任何让我后悔的事”：用户对家用 DNA 检测公司的感知
CHI	2020	预测信息披露的在线隐私启发式规则
CHI	2020	了解急诊科的网络安全实践
CHI	2021	“你得注意自己说的话”：对与在押人员通信的监控
CHI	2021	了解向“黑人的命也是命”抗议者提供的安全与隐私建议
CHI	2021	PriView——探索支持用户隐私的可视化
CHI	2021	“我.....录入了鼻纹，但识别并不准确”：上肢功能障碍者如何在个人设备上进行身份验证计算设备
CHI	2021	为“我们”而构建：面向有记忆问题的伴侣的安全设置
CHI	2021	在老年社区中培训并融入网络安全守护者。
CHI	2021	令人烦恼、令人不安和怪异之处：将电话号码用作标识符以及电话号码回收再利用带来的挑战
CHI	2021	邻里守望：运用推测性设计探索家庭能源交互中的削减与同意相关价值观
CHI	2021	“断开这种联系真的很难”：错失恐惧症在用户不情愿的隐私行为中的作用
CHI	2021	LociMotion：迈向在单次会话中学习强认证密钥
CHI	2021	智能家居个人助理的隐私规范
CHI	2021	Shing：一款具备共情沟通能力的对话代理，用于提醒客户注意疑似在线支付欺诈
CHI	2021	Vid2Doppler：从视频合成多普勒雷达数据，用于训练隐私保护活动识别
CHI	2021	‘Unmochon’：一款打击通过 Facebook Messenger 进行在线性骚扰的工具
CHI	2021	探索以用户为中心的安全设计，以实现易用的身份验证仪式
CHI	2021	PrivacyMic：利用不可听频率进行隐私保护日常活动识别
CHI	2021	披露还是不披露：考察老年人与年轻人的隐私决策过程
CHI	2021	评估 MyData情景：伦理、担忧与前景
CHI	2021	“他们认为在互联网上与陌生人交谈完全没问题”：教师对青春期前儿童在线风险的看法与缓解策略
CHI	2021	你的照片太搞笑了，以至于我不介意通过共享它来侵犯你的隐私：个人幽默风格对在线照片分享行为
CHI	2021	赋能式顺从：有个应用程序就能解决
CHI	2021	隐性具身选择：生物识别监控下的决策与隐私局限
CHI	2021	“如果你选了一个穿裙子的粉色机器人，他们就会看出你是女孩”：儿童如何理解数据处理的定性研究与数字隐私风险
CHI	2021	论智能手机用户理解隐式身份验证的困难
CHI	2021	切换开关、美元符号和三角形：如何（不）有效地通过图标和链接文本传达隐私选择
CHI	2021	人工智能系统在收集用户个人信息时应如何与用户交流？角色框架和自我指涉的影响娱乐主管人机交互
CHI	2021	通过电刺激肌肉进行用户身份验证
CHI	2021	可视化交互式隐私政策：更好的选择？
CHI	2021	RepliCueAuth：验证基于实验室的虚拟现实设置在评估身份验证系统中的应用
CHI	2021	我们与他们（以及它）：美国的社会取向、隐私顾虑与对疫情追踪应用的预期使用情况
CHI	2021	通过众包为增强现实中文本内容的情境适配提供设计指导
CHI	2021	越醒目越好：通过突出且简洁的隐私告知提升用户意识
CHI	2021	抗击传播应用：三大洲用户对 COVID-19 相关智能手机应用的隐私影响认知与接受度
CHI	2021	通过行为生物识别及身体归一化的影响，理解虚拟现实中的用户识别
CHI	2021	我不需要专家！让 URL 钓鱼特征通俗易懂
CHI	2021	数字安全困境：COVID-19 期间亲密伴侣暴力的计算机介导的计算机安全干预分析COVID-19
CHI	2021	“金钱让世界运转”：从开发者视角识别儿童应用程序中提升隐私保护的障碍
CHI	2021	静态分析工具中的安全通知：开发者的态度、理解程度及采取行动的能力
CHI	2021	Auth+Track：通过持续跟踪用户，实现智能手机上的免身份验证交互
CHI	2021	真心话还是大冒险：理解并预测用户如何在网上撒谎并提供不实数据
CHI	2021	更好玩、更有趣、更强大：运用游戏化方法引导人们选择更难预测的图形密码
CHI	2021	比较人力支持与技术支持在接触者追踪中的不同视角
CHI	2021	忽视情境：默认选项和框架效应如何减少智能家居隐私决策中的审慎思考?
CHI	2021	探索隐私保护计算在开发过程中的设计与治理挑战
CHI	2021	床垫下的比特：了解加密资产用户不同的风险认知与安全行为
CHI	2021	“它没有给我拒绝的选项”：对智能家居中安全与隐私用户体验的纵向分析产品
CHI	2021	软件团队中的隐私倡导者：了解他们的动机、策略与挑战
CHI	2021	基于肌肉记忆的具身密码设计空间研究
CHI	2021	调查安全与安保关键事件后汽车驾驶员的信息需求
CSCW	2017	安全能否成为一种常规？敏捷软件开发团队中的组织变革研究
CSCW	2017	什么（或谁）是公开的？隐私设置与社交媒体内容分享
CSCW	2017	父母就是不理解：青少年为何不与父母谈论自己的在线风险经历
CSCW	2017	“这会带来很多工作。”——作为个人数字遗产的一部分，如何应对文件和密码的转移
CSCW	2017	开放协作中的隐私、匿名性与感知风险：对 Tor 用户和维基百科编辑的研究
CSCW	2017	审视观看者：社交网络中出版商的诉求与观看者的隐私担忧
CSCW	2017	公民科学中的隐私考量：开放性环境下的伦理研究
CSCW	2017	在线行为广告的民间认知模型
CSCW	2017	隐私行为对社会影响的易感性：同伴与权威来源
CSCW	2018	孟加拉国共享手机使用中的数字隐私挑战
CSCW	2018	从民用文化转向军事文化的挑战：通过信息与通信技术实现高度选择性披露
CSCW	2018	数字技术与亲密伴侣暴力：一项涉及多个利益相关者的定性分析
CSCW	2018	“密码不能随便告诉别人，因为它们是隐私”：了解儿童对在线隐私与安全的心智模型
CSCW	2018	混淆作为照片分享隐私增强技术的有效性及用户体验
CSCW	2018	这事你会发到 Slack 上吗？安全与隐私对合作式新闻编辑部工作的影响
CSCW	2018	匿名戒酒会与匿名戒毒会中的在线匿名性解读
CSCW	2018	通过设计工作手册探索隐私未来，引发价值观反思

会议	Year	标题
CSCW	2018	“我们的隐私必须不惜一切代价得到保护”：亚马逊土耳其机器人工作者的隐私体验
CSCW	2018	朋友和专家对物联网场景中隐私决策的影响
CSCW	2018	超越隐匿：数据匿名化的组织方法
CSCW	2018	Alexa，你在听吗？智能音箱的隐私认知、担忧与隐私寻求行为
CSCW	2018	在你直播我之前告诉我：管理电子游戏直播中的信息披露
CSCW	2018	当社交网络服务隐私设置变得细化：探究用户选择、理由及其对社交体验的影响
CSCW	2018	区分群体隐私与个人隐私：群体推断技术对隐私认知的影响及行为
CSCW	2018	“我就知道好得不真实”：经济弱势用户在评估可信度时面临的挑战，避免诈骗，并培养在线自我效能
CSCW	2018	用户对智能家居物联网隐私的认知
CSCW	2019	平常且简单：工作场所中的账户共享实践
CSCW	2019	实用工具还是人际关系的阻碍：探究为何一些社交媒体用户避用隐私功能
CSCW	2019	“隐私不是一个概念，而是一种生活方式”：跨国技术平台的本地化与阈限隐私柬埔寨的实践
CSCW	2019	为社区监督开展协同设计：帮助人们共同做出隐私与安全决策
CSCW	2019	“成为更宏大整体的一部分”：面向消费者的基因检测、隐私与个人信息披露
CSCW	2019	“我的手机被黑了吗？”：与亲密伴侣暴力幸存者共同分析临床计算机安全干预措施
CSCW	2019	智能家居中旁观者的隐私认知与设计
CSCW	2020	“这样比引发冲突容易”：在社交媒体上维护社会规范与隐私的制裁策略
CSCW	2020	基于图形用户界面的示例编程系统中的保护隐私的脚本共享
CSCW	2020	有形隐私：面向旁观者隐私的以用户为中心的传感器设计
CSCW	2020	跨性别时光：跨性别者专属社交媒体网站上的安全、隐私和内容警示
CSCW	2020	社会规范脆弱性及其对在线社区中隐私与安全的影响
CSCW	2020	专家如何识别网络钓鱼诈骗邮件
CSCW	2020	为艾滋病病毒感染者设计同伴数据共享平台时对信任、身份、隐私和安全的考量
CSCW	2020	创客空间中的访问与控制之间的张力
CSCW	2020	与青少年开展高风险研究：通过协同设计确保青少年的伦理对待与保护
CSCW	2020	致力于在老年人社区中建立社区集体效能，以管理数字隐私与安全
CSCW	2021	“我们甚至向邻居借了钱”：从受害者经历的角度理解基于移动设备的诈骗
CSCW	2021	拥有与共享：智能音箱用户的隐私认知
CSCW	2021	当强制协作成为最明智的选择：预防性与威慑性机制管理的可取性多方隐私冲突
CSCW	2021	个体脆弱，集体安全：有老年人的家庭的安全与隐私实践
CSCW	2021	如何避免衡量社交网络隐私：一项跨国调查
CSCW	2021	Anshimi：首尔女性对安全数据的认知及安全应用程序的有效性
CSCW	2021	保护与展现：在线视频游戏玩家的姓名、隐私与边界协商
CSCW	2021	“共享是我们共同的责任”：恋爱伴侣账户共享的演变
CSCW	2021	PrivacyPrimer：迈向保护隐私的老年人情景记忆支持
CSCW	2021	张力与缓解措施：理解公共卫生紧急事件中智能手机数据收集相关的顾虑与价值观
CSCW	2021	共享现实：重构体验中的虚拟形象识别与隐私顾虑
CSCW	2021	集体隐私管理实践：对私人 Facebook 群组中隐私策略与风险的研究
CSCW	2021	家庭沟通：探究父母与青少年对在线安全沟通的不同认知
CSCW	2021	隐私研究中衡量文化的难题
CSCW	2021	德国寻求庇护者的数字隐私认知
CSCW	2021	在科技照护这一更广泛的情境中探究隐私与安全方面的协作支持
CSCW	2021	COVID-19 疫情期间隐私相关信任对群件应用的采纳与使用的差异化影响
CSCW	2021	你难道不为他人着想吗？智能手机应用权限中的相互依存隐私
CSCW	2021	智能家居中的儿童安全：父母的看法、需求与缓解策略
CSCW	2021	组织结构和技术使用对计算机应急响应团队协作实践的影响：一项实证研究
SOUPS	2017	面向 GitHub 用户的安全开发者研究：探索便利抽样
SOUPS	2017	“.....使用锁屏总比担心节省几秒钟时间更好”：恐惧诉求在智能手机锁定行为情境中的影响锁定行为
SOUPS	2017	DigiTally：为手机试行离线支付
SOUPS	2017	自动驾驶汽车与数据收集：联网自动驾驶汽车的隐私认知
SOUPS	2017	使用情境调查探索安卓运行时权限对话框中的决策
SOUPS	2017	Replication: 使用数据日志验证钓鱼检测能力指标所面临的挑战
SOUPS	2017	对银行员工信息安全与网络钓鱼体验的定性研究
SOUPS	2017	移动中的身份验证：评估移动对移动设备击键动态特征的影响
SOUPS	2017	新自我：了解专家与非专家对 Tor 匿名网络的认知与使用情况
SOUPS	2017	儿童反网络钓鱼培训的效果如何?
SOUPS	2017	用户特征对自动移动应用程序更新态度的影响
SOUPS	2017	物联网世界中的隐私期望与偏好
SOUPS	2017	我们能否通过社会手段应对社会工程攻击？评估社会显著性在提升钓鱼检测效果方面的作用
SOUPS	2017	评估朋友的隐私：共享个人数据时的匿名性是否重要?
SOUPS	2017	可见性对传感器数据民间理论的重要性
SOUPS	2017	权衡情境与取舍：郊区成年人如何选择其在线安全态势
SOUPS	2017	拉开帷幕：对定向的认知如何影响消费者态度与购买意向
SOUPS	2017	格式与内容：风险与呈现方式对披露决策的影响
SOUPS	2017	多样化以求生存：通过自适应策略增强密码强度
SOUPS	2017	TurtleGuard：帮助安卓用户应用情境隐私偏好
SOUPS	2017	是你吗，Alice？安全即时通信应用身份验证流程的可用性研究
SOUPS	2017	智能家居中的终端用户的安全与隐私顾虑
SOUPS	2018	伦理初现：虚拟现实中的隐私与安全认知故事
SOUPS	2018	软件开发生命周期中的安全
SOUPS	2018	开发者也值得获得安全警告：集成式安全建议对密码学 API 误用的影响
SOUPS	2018	密码过期策略下的用户行为与态度
SOUPS	2018	远离窥探的目光：分析隐私浏览的使用情况与认知

会议	Year	标题
SOUPS	2018	“我们会把这件事看得很重要”：开发加密产品的组织中的安全思维
SOUPS	2018	“这很吓人……令人困惑……也很乏味”：网络安全倡导者如何克服人们对安全的负面看法
SOUPS	2018	编程经验可能无助于高效理解经过混淆处理的源代码
SOUPS	2018	数据泄露：用户对暴露数据的理解、预期及处理方面的担忧
SOUPS	2018	描述基于浏览器的拦截扩展在防止在线跟踪方面的使用情况
SOUPS	2018	在线隐私与数字遗留物的老化
SOUPS	2018	“如果我按下删除，它就消失了”——用户对在线数据删除和过期的理解
SOUPS	2018	开发者密码研究中的欺骗任务设计：探索学生样本
SOUPS	2018	介绍网络生存任务：评估并解决员工对有效网络安全防护的信念
SOUPS	2018	非正式支持网络：对家庭数据安全实践的调查
SOUPS	2018	API盲点：经验丰富的开发者为何会编写易受攻击的代码
SOUPS	2018	分享与共享？浪漫关系中的安全行为探究
SOUPS	2018	数字人脸变形能否影响态度和在线行为?
SOUPS	2018	恐惧诉求对提升沙特阿拉伯人智能手机锁定行为的有效性
SOUPS	2018	“你不想成为下一个表情包”：大学生在无处不在的摄影时代管理隐私的变通做法
SOUPS	2018	安全电子邮件密钥管理的可用性比较研究
SOUPS	2018	需要采取行动！帮助用户在 Signal 中找到并完成身份验证流程
SOUPS	2018	重复研究：关于自动取款机及各种电子支付情景
SOUPS	2018	不同情境下用户对安卓后台资源访问的接受度
SOUPS	2018	树何时才真的是卡车？探索加密的心智模型
SOUPS	2018	“我没什么可失去的”：Equifax 数据泄露事件后消费者的风险认知与防护行为
SOUPS	2018	“隐私不是为我准备的，而是为那些富裕女性准备的”：南亚女性在移动电话上的表演性隐私实践
SOUPS	2019	不只是智能音箱：智能家居个人助理的安全与隐私认知
SOUPS	2019	“没有什么是我需要保密的”：可穿戴健身数据的共享实践与担忧
SOUPS	2019	评估用户对系统隐私的认知：区分社会层面与制度层面
SOUPS	2019	Replication: 没人能入侵我的思想：重新审视一项关于专家与非专家的安全实践和建议的研究
SOUPS	2019	对双因素心存疑虑：通过设备比较和经验抽样，了解 FIDO U2F 在日常使用中的可用性
SOUPS	2019	终端用户安全与隐私行为的感知触发因素类型学
SOUPS	2019	终端用户安全态度的自我报告测量（SA-6）
SOUPS	2019	老年人的隐私与安全威胁模型及缓解策略
SOUPS	2019	娱乐媒体对计算机安全心智模型的影响
SOUPS	2019	协作式隐私与安全：向视力障碍者及其盟友学习
SOUPS	2019	通过交互式按需增量信息披露界面增强隐私：将隐私保护设计应用于记录链接
SOUPS	2019	机器的守护者：探究系统管理员如何管理软件更新
SOUPS	2019	探索移动触屏设备上的密码输入有意行为改变
SOUPS	2019	在移动端连续认证系统中传达设备置信度和即将进行的重新认证设备
SOUPS	2019	“我们离不开它们！”应用开发者对广告网络的采用及其对消费者风险的考量
SOUPS	2019	为什么人们（不）能有效地使用密码管理器
SOUPS	2019	从可用性到安全计算，再回到可用性
SOUPS	2019	五种双因素认证方法的可用性研究
SOUPS	2019	“有人告诉我，要么购买软件，要么失去电脑。我没理会”：一项关于勒索软件的研究
SOUPS	2019	“数据不属于我”：终端用户对智能家居设备数据实践及风险的认知
SOUPS	2019	警告迷雾：非必要通知如何与安全警告混淆
SOUPS	2019	系统管理员更喜欢命令行界面，不是吗？防火墙界面的探索性研究
SOUPS	2019	“有些东西不安全，但我不确定这会造成什么问题”：通过设计促进理解，增强自主性，应用于 Signal
SOUPS	2020	“你已经列出了漂亮的漏洞清单，接下来呢？”现实中的漏洞发现与管理流程
SOUPS	2020	隐私与安全对每个人都重要吗？量化和聚类分析有关智能家居设备的以用户为中心的考量采用
SOUPS	2020	硬件逆向工程技术与认知流程的探索性研究
SOUPS	2020	创新停滞还是积极行动？用户体验在智能家居摄像头安全与隐私设计中的作用
SOUPS	2020	真实用户的 IFTTT 应用程序有多大风险？
SOUPS	2020	Replication: 在线安全开发者研究的生态效度：探索在密码存储研究中对自由职业者的欺骗
SOUPS	2020	从比较沙特与印度人群的 WhatsApp 隐私顾虑中获得的经验
SOUPS	2020	盲人与普通人：探索更易用的音频 CAPTCHA 设计
SOUPS	2020	“你最终还是用了密码”——探索小型公司的 FIDO2 安全密钥
SOUPS	2020	可用性性安全：研究人们发送性短信时的顾虑与策略
SOUPS	2020	通过隐私告知的视觉设计提升隐私：探索好奇心、控制与情感之间的相互作用
SOUPS	2020	用户对加密货币系统的心智模型——一种扎根理论方法
SOUPS	2020	实现选择：为应对认知障碍的伴侣提供在线保障措施
SOUPS	2020	行业对欧盟《网络与信息系统安全指令》（NIS）的响应：理解政策关键基础设施中的实施实践
SOUPS	2020	迈向理解在线性侵害举报中的隐私与信任
SOUPS	2020	“我的思维过程很狭隘”：连接推断与自我认知的解释所面临的约束
SOUPS	2020	敲，敲。谁在那儿？论 LG 敲击码的安全性
SOUPS	2020	为什么 Johnny 无法修复漏洞：面向安全的静态分析工具可用性评估
SOUPS	2020	从意图到行动：助推用户使用安全的移动支付
SOUPS	2020	安全性、可用性与多种信息来源：探索系统管理员的更新行为
SOUPS	2020	阴云密布，误解时有发生：探索用户对云办公套件中安全与隐私的用户的认知与期望套件
SOUPS	2021	比较美国不同智能手机和智能音箱平台用户的安全与隐私态度
SOUPS	2021	Replication: 媒体对技术用户心智模型的影响
SOUPS	2021	“我完全不知道他们想要做什么”：热情用户和普通 Signal 用户对 Signal 个人识别码的理解
SOUPS	2021	审视审查者：学生对在线监考服务的隐私与安全认知
SOUPS	2021	“这东西没有名字”：从智能家居安全领域涌现的真实世界干预措施中学习

会议	Year	标题
SOUPS	2021	忧心忡忡却无能为力：清理待处置旧设备时的用户认知、方法与挑战
SOUPS	2021	PowerCut 与 Obfuscator：智能音箱隐私保护干预措施设计空间探索
SOUPS	2021	迈向易用且安全的基于位置的智能手机身份验证
SOUPS	2021	虚拟课堂与现实伤害：美国大学的远程学习
SOUPS	2021	将代码审查作为与开发者开展在线安全研究的方法论——关于自由职业者密码存储的案例研究
SOUPS	2021	了解 COVID-19 疫情期间人们对远程通信的隐私态度与担忧
SOUPS	2021	采用安全编程语言的优缺点：以 Rust 为案例研究
SOUPS	2021	请勿使用 !? 或您的车牌号码：德国公司的密码策略分析
SOUPS	2021	通过情境化理由评估并重新定义移动增强现实应用程序的智能手机权限
SOUPS	2021	绝不使用，还是无论如何都会使用：探究德国用户采用 Corona-Warn-App 的意愿及其误解
SOUPS	2021	他们为何忽视英文电子邮件：非母语者识别网络钓鱼邮件所面临的挑战
SOUPS	2021	了解用户对浏览器扩展隐私与安全的认知
SOUPS	2021	“我如何确定”：人们对完全自动化决策（SADM）的看法
SOUPS	2021	面向多元视角设计有害内容分类
SOUPS	2021	使用黑名单提升用户选择安卓图案的安全性
SOUPS	2021	“我真的只是希望这能奏效”：阻碍视觉障碍用户在线安全与隐私的障碍
SOUPS	2021	大规模远程办公的挑战与威胁：对工作者的定性研究
SOUPS	2021	用户对智能手机作为 FIDO2 漫游认证器的可用性和安全性的认知
SOUPS	2021	针对计算机科学专业学生和 CTF 玩家的 Clang 静态分析器与 libFuzzer 定性可用性评估
SOUPS	2021	探索智能家居语音助手上安全敏感任务的身份验证
SOUPS	2021	论加密可视化的有限影响：对端到端消息安全的认知
SOUPS	2021	决定个性化广告：通过助推提升开发者对用户隐私的关注
SOUPS	2021	通过协同设计，依据《通用数据保护条例》/《加州消费者隐私法》的访问权，打造易用且实用的数据下载功能
SOUPS	2021	非专业用户在网络钓鱼检测中运用的知识与能力
SOUPS	2021	“这是否合乎道德是另一回事”：消费者对隐私法规和企业数据实践的看法
SOUPS	2021	人脸识别：了解日益多样化部署场景中的隐私顾虑与态度
SOUPS	2021	WebAlly：让视力障碍人士也能使用基于视觉任务的验证码
USEC	2017	使用认知心理学的方法在单次注册会话中学习系统分配的密码（最多 56 比特）
USEC	2017	EmojiAuth：量化基于表情符号的身份验证的安全性
USEC	2017	在存在黑名单的情况下创建密码
USEC	2017	无缝且安全的虚拟现实：为虚拟现实调整并评估成熟的身份验证系统
USEC	2017	我不使用 Apple Pay，因为它不够安全.....：移动轻触支付中的安全性与可用性感知
USEC	2017	做好准备：美国政府专家如何看待网络安全
USEC	2017	探索可穿戴设备隐私的设计方向
USEC	2018	探索网站位置作为安全指标的作用
USEC	2018	安全运营中心中的声化：安全从业者怎么看?
USEC	2018	TinPal：图案锁的增强型界面
USEC	2018	探究安全/隐私态度与解锁身份验证之间的关联
USEC	2018	量化用户对软件更新的看法
USEC	2018	对伊朗 Telegram 用户的隐私偏好与实践的调查
USEC	2018	隐喻是否有害？对功能性隐喻在端到端加密中的有效性进行的一项探索性研究
USEC	2018	探究家长的安全与隐私顾虑及实践
USEC	2019	Replication: 如果不会输，我们还会打盹吗？在习惯化用户研究中利用激励对风险进行建模
USEC	2019	当安全受到欢迎时：探索设备购买作为安全行为改变的契机
USEC	2019	网络犯罪调查人员也是用户！了解执法部门面临的社会技术挑战
USEC	2019	拥有控制却无法控制：Windows 10 家庭版更新功能的认知与现实
USEC	2019	这个应用程序尊重我的隐私吗？支持智能手机用户做出隐私相关决策的信息材料的设计与评估
		智能手机用户
USEC	2019	他们会共享吗？通过对过去隐私行为的自我反思预测智能手机用户的位置共享行为
USEC	2019	设计一款支持隐私决策社会过程的移动应用程序
USEC	2019	初探 OpenVAS 漏洞扫描器的可用性
USEC	2019	从顶部解锁——提升安卓解锁图案的安全性
USEC	2019	使用腕带进行持续的智能手机身份验证
USEC	2019	案例研究——探索儿童的密码知识与实践
USEC	2020	以用户为中心的风险沟通，助力更安全的浏览
USEC	2020	外包员工成为信息系统安全威胁来源的行为
USEC	2020	将共情作为应对密码选择挫折的一种方式
USEC	2020	探索听觉刺激对 CAPTCHA 性能的影响
USEC	2020	我们信任雇主：办公室职员隐私认知的心智模型
USEC	2020	修复修复方案：评估 SAST 工具在保障密码存储安全方面的解决方案
USEC	2020	浏览器之争：理解韩国用户的网络浏览器选择
USEC	2020	理解人们对智能设备的看法
USEC	2020	在线失权：对隐私与共享看法及方法偏好的调查
USEC	2020	线索利用与认知负荷对网络钓鱼邮件检测的影响
USEC	2020	PassPage：一种基于网络浏览记录的图形密码身份验证方案
USEC	2020	智能环境中的安全与隐私意识——一项跨国调查
USEC	2020	线索利用、网络钓鱼特征与网络钓鱼邮件检测
USEC	2020	安全电子邮件——一项可用性研究
USEC	2021	提升食品供应链中的信任
USEC	2021	加密货币钱包的整体隐私与可用性
USEC	2021	程序员为什么会做他们所做的事？影响安全实践的因素理论
USEC	2021	“丢了手机，就丢了身份”：探讨用户对数字身份服务的认知与期望
USEC	2021	网络钓鱼抵御能力跨国研究
USEC	2021	我的过去决定我的现在：纵向数据在 Facebook 上的相关性、暴露与影响
USEC	2021	基于情境的安全高管层级网络风险认知评估
EuroUSEC	2017	我想进行一场辩论，请用辩证法提升应用安全的成效
EuroUSEC	2017	Pass-Roll 和 Pass-Scroll：用于改进文本密码的新型图形用户界面
EuroUSEC	2017	聊天世界的安全保护伞：对 Telegram 的分析评估和用户研究
EuroUSEC	2017	在组织文化融合中寻找安全倡导者

会议	Year	标题
EuroUSEC	2017	个性化安全消息：助推用户遵守浏览器警告
EuroUSEC	2017	信息安全风险可视化对管理者决策的影响
EuroUSEC	2017	通过移动设备运动传感器泄露信息：用户意识与担忧
EuroUSEC	2017	我做到了，也理解了。安全 API 尚非如此。真遗憾
EuroUSEC	2017	Johnny 能构建协议吗？协调开发者与用户的意图，打造增强隐私保护的安全消息协议
EuroUSEC	2017	Pico 实战：逐个网站替换密码
EuroUSEC	2017	什么是安全电子邮件?
EuroUSEC	2018	权限不可能：在游戏环境中教授防火墙配置
EuroUSEC	2018	用户对删除即时消息的感知与预期——或者说：“如果我按下这个按钮，会发生什么？”
EuroUSEC	2018	“Retailio”隐私向导：协助用户设置智能零售商店的隐私设置
EuroUSEC	2018	重新思考家庭网络安全
EuroUSEC	2018	“本网站使用 Cookie”：用户对 Cookie 免责声明的认知与反应
EuroUSEC	2018	隐私侵犯在隐私权衡中的作用
EuroUSEC	2018	“数据不能用于什么用途？”美国用户对智能电视的隐私期望
EuroUSEC	2018	安全电子邮件删除的可用性研究
EuroUSEC	2019	2 Fast 2 Secure：数据泄露后的安全变更案例研究
EuroUSEC	2019	三个语言圈的比较分析：语言与文化差异是否体现在密码选择习惯中?
EuroUSEC	2019	“别惩罚我们所有人”：衡量用户对双因素认证的态度
EuroUSEC	2019	严肃游戏如何助力安全编程？研究复现与干预的设计
EuroUSEC	2019	Johnny为何无法保护自己的隐私
EuroUSEC	2020	《通用数据保护条例》现实检验——向公司索取并调查个人身份识别数据
EuroUSEC	2020	保守社会中的女性是否会遵循智能手机安全建议？沙特阿拉伯和巴基斯坦的案例研究
EuroUSEC	2020	终端用户和专家对威胁及潜在对策的认知
EuroUSEC	2020	提升非专家对端到端加密的理解：一项探索性研究
EuroUSEC	2020	现金、银行卡还是加密货币？四个国家的支付文化研究
EuroUSEC	2020	让加密更令人安心：探究加密描述如何影响感知安全
EuroUSEC	2020	模拟社会临场感对金融自动化机器人中的信任、隐私顾虑与使用意向的影响
EuroUSEC	2020	调查青少年识别网络钓鱼信息的能力
EuroUSEC	2020	移动应用中的数据共享——欧洲的用户隐私预期
EuroUSEC	2020	“安全应当默认启用”：调查记者如何看待并应对物联网带来的风险
EuroUSEC	2020	技术之痛：网络安全体验的亲历描述
EuroUSEC	2021	在德国复现一项关于勒索软件的研究
EuroUSEC	2021	找到秘密宝藏？通过游戏化改进记忆型秘密
EuroUSEC	2021	使用参与式工具包探究青少年对职场隐私的看法
EuroUSEC	2021	Replication: 衡量德国用户对智能手机安全与隐私的认知
EuroUSEC	2021	Microsoft Office 宏警告：一场设计错误喜剧及其悲剧性的安全后果
EuroUSEC	2021	考察移动应用程序意图使用与实际使用之间的电量使用和隐私悖论
EuroUSEC	2021	助推还是约束：人如何评价网络安全中的助推——德国的一项代表性研究
EuroUSEC	2021	粗心的参与者对我们的网络钓鱼研究至关重要：了解筛选方法的影响
EuroUSEC	2021	什么泄露事件？通过研究现实世界中的浏览行为，衡量人们对安全事件的在线认知
EuroUSEC	2021	即插即用：网络安全远程实验框架
EuroUSEC	2021	比较文本式与视频式传达在激励用户采用密码管理器方面的效果
EuroUSEC	2021	了解年轻人的网络安全体验
EuroUSEC	2021	窥探黑箱：深入理解用户对端到端加密的认知