

儿童和互联网

互联网是当今文化日益重要的组成部分，对儿童和青少年来说尤其如此，学校作业、在线游戏和社交网络是最受欢迎的一些活动。但是，在教育和保护儿童的正确方式方面缺乏共识，令儿童的在线体验和表达面临更多挑战。此外，法律和社会规范方面的文化和地域差异反映了一个事实，即在“儿童的定义是什么”或者“什么对儿童是适当的”等问题上没有普遍接受的观点，从而难以界定“不适当的内容和行为”。

虽然一些网络犯罪具有跨国性质并因此需要全球关注；但在国家层面上，监管内容的政策性方法迄今为止主要使用的是一系列过滤技术来限制访问或拦截互联网内容。此外，虽然常常建议采用当地机构或单个家庭计算机级别的过滤（而且原则上应优先于网络级别过滤），但无论是这些努力还是国家和地方级别的过滤方法对监管不良内容都不是100%有效的，因为有时它们倾向于过度拦截内容或拦截不足。网络级别的过滤则有额外的不利影响。因此，家长、教育工作者、监护人、同龄人和国家对儿童和青少年进行有关使用互联网时可能面临的风险和责任方面的教育是至关重要的。这种方式可使青少年能够认识和规避危险，同时培养他们的上网技能，以便他们以负责任的方式从互联网活动中获得益处。

简介

对儿童和成年人来说，互联网都是极其重要的媒体。当今的儿童和青少年经常为了以下目的使用互联网：

- 学习（通过接触信息、知识、见解、教育工具甚至教师）；
- 沟通（表达思想，分享信息和经验）；
- 与朋友和同龄人进行社交互动；
- 创新、创造和分享内容；
- 玩耍和娱乐（游戏、电影、音乐、书籍等）；

这些活动越来越多地在家庭或学校以外进行，并且不只在传统台式计算机上进行，还在诸如智能手机和平板电脑这样的手持设备上进行。

与其他内容提供技术（如广播和电视）相比，互联网为家长、监护人和教育工作者提供了独特的机会，能够更直接地决定自己的孩子可以看什么和做什么。例如，他们可以根据每名儿童的年龄、文化、智力和受教育程度等，引导儿童接触适合他们的有益和有趣的内容。互联网也让人们有机会来教育儿童要建设性地利用互联网以及指导儿童如何规避有风险的上网行为和不当的内容。

所有人（家长和监护人、教师、机构和政府）共同努力为儿童和青少年营造安全和便利的环境是至关重要的，无论他们身在何处：在家、在学校，或在诸如图书馆或网吧等公共场所中。每个人都有责任营造这样的环境，以便所有儿童和青少年都能享受和利用互联网的积极方面。

此外，虽然务必要注意与儿童上网相关的潜在风险，但也务必要全面正确地看待事物。最好从教育、常识和明确的准则着手。虽然关于如何更好地保护儿童已经做了许多工作，但是互联网协会认为还可以做更多事情来为儿童和青少年增权赋能，以保护他们免受互联网上潜在有害资料的影响，同时使他们能够充分利用互联网的功能和价值。

“儿童”的定义是什么？

确定儿童的定义是最具挑战性的问题之一，因为根据社会和学科定义的不同，确定方式也截然不同。

联合国《儿童权利公约》(CRC) 第1条规定：“儿童系指18岁以下的任何人，除非对其适用之法律规定成年年龄低于18岁。”尽管该定义的出发点是好的，但把年龄限制设置为18岁从许多方面来讲可能是值得商榷的。

当然也存在“儿童”的其他定义，但每个定义都从不同的科学角度来定义“儿童”一词。例如，心理学采用与心理成熟和发展相关的某种标准，而生物学则偏向于采用与身体发育相关的标准。从非科学的角度来看，伦理学者在确定儿童的定义时支持采用“道德心和同意自由”的概念。

儿童对互联网的使用

在儿童的定义标准方面达成一致意见似乎是实现有效儿童保护的最大障碍之一。但无论我们如何定义这一词汇，我们当然都知道，儿童和青少年经常使用互联网，因为互联网已成为现代生活的一个基本组成部分。儿童访问互联网的能力迅速增强，并且大多数青少年都频繁访问互联网。

儿童在互联网上参与各种各样的活动，并且许多活动都同时进行，因为Web 2.0平台日益成为当今青少年文化的一部分。一项由欧洲委员会“网络安全计划”资助并由欧盟儿童在线进行的25国调查结果显示，儿童和青少年使用互联网进行的一些首要活动是：学校作业(92%)、玩游戏(83%)、观看视频片段(75%)和社交(71%)。59%使用互联网的欧洲儿童拥有自己的社交网络个人资料。9-10岁儿童中只有28%拥有社交网络个人资料，但在11-12岁青少年中这个比例高达59%，这表明使用社交网络的主要触发因素是开始接受中学教育，而不是各个主要提供商设定的最低年龄限制。¹为此，确定和建立能够引导在线互动交流的规范应成为儿童教育不可分割的组成部分，并且必须从小学低年级开始。

确保儿童网络安全的要素之一是帮助他们理解网络风险和安全的概念，这将让儿童能够在充分知情的基础上独立做出决定。互联网安全教育在保护青少年免受以下网络威胁的危害时是至关重要的：外部威胁，如“不适当的”内容和活动（如赌博）或与“错误的”人员联系（如欺凌、尾随、诈骗）；以及内部威胁（如泄露太多个人信息）。通过与儿童携手合作、倾听他们的需求和学习他们的经验，我们能够为孩子营造一个良好的环境，使他们能够在以安全和负责任的方式行事的同时，充分利用互联网提供的机会。同时，这类环境能够帮助那些利用互联网来做“坏事”的儿童了解自己的行为对更弱势对象产生的实际影响。

最后，务必要记住，互联网不是一个使儿童面临前所未有危险的“邪恶”工具。这个观念符合允许犯错误的思想派别，该派别说明了为何“保持适应能力（在达成曾经的核心目标的同时适应已变化环境的能力）在这样一个充满不可预见的混乱和动荡的时代是一项基本技能”。²基于这一理论，在保护儿童网络安全方面，立法和监管可能到头来适得其反。试图禁止可能使儿童面临网上危险的所有活动是不可能的（并且可能是徒劳的）；一个更健康、允许犯错误的方式是把教育和增权赋能看作使家长、教育工作者或国家能够解决与儿童网络安全相关的此类问题的工具。我们应力求循序渐进地让孩子接触互联网，并使用允许犯错误的弹性策略来教导他们如何应对互联网环境及其危险。为此，把“网络礼仪”的重要性告诉孩子以及向他们灌输“三思而后点击”的理念应是我们的首要目标。

出于这种考虑，以下章节说明了儿童在网上面临的一些危险。

¹可访问以下网址查看更多统计数据：<http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx>

² Andrew Zolli & Ann Marie Healy (2012). “*Resilience: Why Things Bounce Back*”, Free Press,

儿童虐待和儿童色情的定义相关问题

在《关于贩卖儿童、儿童卖淫和儿童色情的儿童权利公约任择议定书》中，³国际上第一次尝试将“儿童色情”定义为一种虐待儿童的形式。但欧洲理事会《保护儿童免受性剥削和性虐待公约》⁴（于2007年10月开放以供签署）中的最新定义更为清晰。第20条把儿童色情定义为“直观地描述儿童从事实际或模拟的色情行为或者主要出于性目的而描述儿童性器官的任何资料”。

由于此类行为通常是隐蔽的并且对哪些资料应被列为儿童性虐待资料也缺乏统一的定义，目前尚不清楚此类资料的散布范围有多广泛。世界各地缺乏关于儿童性虐待资料制作和传播方面的数据，而且此类资料的制作和消费全球模式在不断变化，更是加剧了这一困难。数码相机和计算机技术的飞速发展扩大了对此类资料的访问并且使人能够创建以数字方式生成或修改的图像，这使得收集有关此问题规模的可靠统计信息变得更加困难。

此外，缺乏明确宣布儿童性虐待资料为非法的统一全国立法或全球控制措施，也使得儿童网络保护成为一项非常艰巨的任务。只有一些国家或地区出台了宣告儿童性虐待资料为非法的立法。虽然一些国家开始了法律改革进程，但是大多数国家仍依靠过时的立法来打击淫秽，这不足以对付通过互联网进行的性侵犯或性虐待行为。

单是政府层面缺乏对问题规模的明确共识以及缺乏相应的法律对策这一点就足以突显向儿童提供家长引导和教育指导的重要性。务必要确保儿童知道，在使用互联网时如果遇到儿童性虐待资料或可能试图引诱他们陷入危险处境的犯罪者时如何应对。

其他潜在威胁

儿童和青少年在使用电脑时面临各种各样的风险。其中一些风险是对他们安全或隐私的威胁。还有一些风险可能是由于儿童有意或无意地违反法律（如版权或反诽谤法律）引起的。这些风险也可能产生严重后果。⁵

儿童和青少年面临哪些风险？

- 有意或无意地接触不适当的图片或内容。
- 性侵犯者通过聊天室、其他形式的社交媒体以及电子邮件进行教唆。
- 网络欺凌或骚扰。
- 个人信息的不当披露和数据盗窃（通过过度分享或其他方式）。
- 间谍软件、病毒和恶意软件。
- 诈骗
- 过度商业化：广告及与产品相关的网站。
- 被诱惑从事软件、音乐或视频盗版的后果。⁴

青少年是互联网使用人数增长最快的年龄组；但当他们缺乏意识以及风险评估和做决定能力有限时，他们又易受伤害。多方利益相关者在地方、国家和国际层面的合作是一种有效的方式，可增强对世界一些地区儿童保护问题重要性的认识。此外，维持治安需要多方机构在地方和国家层面的合作；而在国际层面，合作和信息共享在儿童保护方面是至关重要的。

在儿童保护方面没有一刀切的办法

在儿童时期形成的概念以及哪些做法是适当的或可接受的想法方面，存在文化和地域差异。在内容方面，具体而言是在“不适当的内容”方面，儿童群体并不是同质的。每名儿童都是不同的：不同的年龄、受教育程度、语言、文化、宗教、成熟度、经历、兴趣等等，并且每名儿童会随着成熟和发

³http://www.unicef.org/crc/index_protocols.html

⁴<http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm>

⁵这类威胁非常显著，但超出本文的讨论范畴。

育而迅速发生变化。确定什么样的内容适合儿童个人，这一任务最好留给了解儿童的家长、监护人和教育工作者来做。

新技术的普及以及围绕它们的政策制定不可避免的滞后，再加之文化多样性和发展水平都凸显了寻找解决方案的复杂性。从积极的一面来看，制作和宣传适合文化、语言和年龄的内容，使之具有吸引力并易于访问是同样重要的。

控制访问不良内容的方法

世界上许多国家都选择制定互联网监管的全国性方式，并获得了不同程度的成功，有时却产生意想不到的后果。可以从近年来单纯限制访问互联网内容的国家数量迅速攀升这一现象中看到这一点。此外，越来越多的国家尝试通过实施互联网过滤这一技术方法来控制对内容的访问。一般来说，以下三种技术被常用于阻止访问网站：IP封锁，DNS过滤及使用代理进行URL拦截。关键字拦截（即根据在请求的URL中找到的关键字来阻止对网站的访问，或者根据一份禁用词列表来阻止搜索）是一种更先进的技术，正被越来越多的国家所采用。这些方法可在不同位置实施；例如，在互联网服务提供商（ISP）、某个机构或特定的上网设备处。

存在许多不同的过滤技术，它们都旨在限制对特定网站的访问。一些技术是基于ISP或有关当局在网络层面上创建和部署的一份“不良网站”列表，但家长、监护人、教育工作者或其他当局也可利用各种程序和工具来监视、追踪和阻止儿童所用的设备上对特定网络活动的访问；例如：

- 可允许或拦截特定网站和协议的代理和软件（包括反病毒防护、垃圾邮件过滤器、弹窗拦截程序、反间谍软件、cookie删除软件等）
- 查找和拦截特定内容或网站的内容过滤软件
- 可设置网站隐私和监控功能的配置选项（例如，谷歌SafeSearch过滤器，Privolock等）

但是，过滤绝不是100%有效的。过滤技术往往有两种简单的固有缺陷：拦截不足或拦截过度。拦截不足是指过滤未能拦截对所有目标内容的访问。另一方面，过滤技术通常会拦截它们不应拦截的内容，这被称为拦截过度。出现这两种缺陷的原因是许多黑名单是通过结合使用手动指定网站和自动搜索产生的，因此常常包含被错误分类的网站。如果其他内容也是由同一IP地址或网域托管，就会出现额外问题。此外，过滤方法并不能去除互联网的非法内容，⁶并且容易被绕过。它们还可能有意或无意地限制自由和开放的沟通交流，从而限制个人或少数群体的权利。

由于网络过滤器常常是专有的和/或使用秘密的“黑名单”，因此在网站的标记和限制方面常常缺乏透明度。如果制作内容过滤技术的公司与不民主的政权携手合作来设置全国范围内的内容过滤计划，这种透明度的缺乏就变得特别令人不安。大多数实施内容过滤和拦截的国家在商业生成的拦截列表基础之上还增加了侧重于特定国家或语言的各个主题和组织的自定义列表。

虽然在校互联网使用通常受到过滤或监管，但许多儿童可从几个不同地点通过不同设备访问互联网，而这些地点或设备中可能不存在过滤器并且几乎没有监管。儿童和青少年越来越多地通过其他上网设备来访问互联网；例如，智能手机、平板电脑和游戏设备等。这意味着，即使过滤被部署在家用电脑或学校电脑中，儿童和青少年可能仍将能够通过其他方式或者甚至可能绕过部署在电脑上的过滤器来访问未经过滤的互联网。因此，务必要在网络行为方面教育孩子，并让他们参与讨论自己可能遇到的问题。

可以说，在网络层面上的过滤（如DNS过滤）也会导致网络不稳定、助长分裂并腐蚀互联网的根基。⁷其他控制内容的方法（如域名扣押，该方法不只是为了保护青少年）也存在DNS过滤所遇到的大多数相同问题（包括容易被规避、未能解决根本问题并助长逍遥法外的影子网络等）。

⁶ 只要几分钟就能建立起另一个指向同样互联网地址的域名。

⁷ 可访问以下网址查看有关DNS拦截的更多信息：<http://www.internetsociety.org/what-we-do/issues/dns/finding-solutions-illegal-line-activities>

虽然软件可能拦截引人注目的特定网站，但没有任何解决方案是经久不衰或完全有效的。技术手段无法在数十亿网站和其他互联网应用（如新闻组、邮件列表、聊天室、即时通讯和社交媒体）中准确地识别和定位特定类别的内容。过滤绝不可取代良好的家长参与和建议。无论如何，这些方法都无法从互联网中去除令人反感或非法的内容；它们只能让这些内容难以被访问。

最后，互联网协会担心儿童网络保护可能是政府借此加强网络控制的大门或后门。所有这一切都表明，拦截内容并不能确保儿童和青少年100%的网络安全。但是，通过赋予儿童、家长、监护人、教育工作者和同龄人识别和处理电脑、互联网和移动电话上的有害内容并且安全和负责任地使用技术的能力，以及通过提供易用的可调整工具来管理访问权限和内容，我们可以提高儿童和青少年的网络安全性。

近期政策指导

经济合作与发展组织于2011年发布了一份题为*儿童网络保护：儿童在网上面临的风险及保护儿童的政策*⁸的报告，并于2012年通过了*儿童网络保护理事会建议*⁹，确立了以下三个主要原则：

- 增权赋能
- 相称性和基本价值观
- 灵活性。

此外，该建议¹⁰呼吁各国政府：

- 通过政策来体现领导作用和承诺；
- 支持所有利益相关者协调一致的应对措施； 促进国内儿童网络保护倡议在所有公私利益相关者中间的一致性和连贯性；
- 把增强意识和教育作为家长和儿童增权赋能必不可少的工具；
- 支持基于证据的儿童网络保护政策；
- 鼓励开发和采用各种尊重儿童权利和其他互联网用户自由的儿童网络保护技术；
- 巩固由致力于儿童网络保护的全国性组织组成的国际网络；
- 分享有关儿童网络保护的国家政策性方式相关信息，特别是为定量和定性的国际性政策比较分析建立经验基础；
- 支持地区性和国际性的能力建设，以改善儿童网络保护的政策和操作措施；
- 更好地协调各个国际性和地区性组织和机构的工作（此类组织和机构在支持政府的该领域工作方面发挥着一定作用），并在适当时候让非政府利益相关者也参与其中。

为儿童增权赋能：家长、监护人和教育工作者的建设性作用

或许，应对已察觉到的互联网使用相关问题的最有效方式是儿童和青少年增权赋能，以便他们知道如何保护自己和朋友。增权赋能技巧包括使用符合他们年龄的措辞，告诉他们有关法律界限的知识，以及坦诚讨论他们所在社区的文化、道德、伦理规范和期望。家长、教育工作者、私营部门、政府和其他人的作用是帮助青少年学会认可和尊重这些界限和规范。为儿童和青少年增权赋能也有助于防止他们成为其他威胁（包括诈骗、间谍软件和恶意软件）的受害者。

虽然家长可使用不断涌现的有效策略来管理儿童对互联网的使用，但儿童规避或抗拒这种家庭监管的策略也层出不穷。与家长相比，儿童常常在使用新媒体时更有信心和有更多的专业知识，这让情况变得更加复杂。但是，当成年人和同龄人的建议和意见得到儿童和青少年的重视时，儿童和青少

⁸http://www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online_5kgcjf71pl28-en

⁹<http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False>

¹⁰<http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False>

年通常就会与他们（“受信任的影响者”）建立信任关系。这些受信任的影响者自身务必要了解潜在的风险和解决方案，并且熟悉如何有效地把信息传达给那些视他们为榜样、信赖他们提供的信息和建议的儿童和青少年。同时也务必认识到这些受信任的影响者会随着时间的推移而改变。随着儿童接近“青春期”，他们的同龄人可能会成为更强大的影响者。

此外，家长、监护人、教育工作者和受信任的影响者都应发挥积极的作用，让儿童和青少年知道他们可能面临来自网络色情资料以及互联网侵犯者和骗子的风险，以及如何避免此类风险。同样重要的是，儿童也应接受有关如何与认识的朋友进行私密交流以及在互联网上分享个人信息时要小心的教育。当然，为了有效地进行教育，家长、监护人、教育工作者和同龄人必须能够熟练使用计算机。

至少有两个因素对家长控制自己子女访问和使用互联网的能力构成挑战。首先，在家长负责子女安全的同时，他们还必须尊重子女日益增长的独立性和隐私权。

其次，很少有家长充分了解子女的互联网文化。¹¹儿童和青少年使用社交网络往往令家长感到困惑。此外，在对待隐私、保密性和个人对自己拥有和分享的数据权利的态度方面，也存在巨大的代沟。安全、隐私、网络侵犯和网络欺凌等问题在技术和心理上都非常复杂，并且家长可能感到难以跟上变化。这些因素表明迫切需要鼓励家长与子女多接触并讨论子女的网络活动，无论家长拥有多少经验。参与其中将使家长、监护人、教育工作者和其他受信任的影响者能够让儿童和青少年免受伤害。

同样重要的是培养儿童的网络技能。这包括教导并鼓励他们掌握信息及通信技术工具以及如何（单独和在团队中）做出正确的决定，以便他们成长为负责任和值得信赖的下一代影响者。

结论

虽然在家庭、学校以及其他允许一对一互动和咨询的环境中可直接与儿童打交道，但是政府、非营利组织和社区组织可采取众多措施来培养意识并建设能力，以帮助儿童和青少年在安全的环境中通过互联网获益。以下举例说明了一些可以考虑的措施：

- 让所有利益相关者参与社区意识培养活动：政府机构、私营互联网部门、非政府组织、社区组织和公众。¹²
- 设立互联网电话热线，以支持公众举报网络犯罪行为并提供咨询和建议。
- 鼓励设立涉及互联网服务提供商和执法机构的教育性计划，以便形成应对非法内容和行为的最佳做法。
- 建立各种网站或平台，为儿童、青少年、家长和教师提供一个教育平台。这些网站应具备有关互联网安全的最新内容并定期更新，以及各种语言版本的自我指导视频。

互联网变化如此之快，以至于技术措施不可能随时跟上。更加有效和持久的措施建立于家庭、社区、教育和增权赋能的基础之上，以便儿童和青少年做出正确选择并从互联网的原动力中获益。

¹¹他们的子女使用互联网和移动电话进行工作、娱乐和社交的方式

¹² 如需了解互联网安全意识网站良好做法的范例，请访问www.kidsap.org和国际终止童妓组织的《安全网络手册》

附录

给家长、儿童和教育工作者的“窍门和小贴士”

以下是家长、教师（和儿童）应该知道的有关互联网使用的一些小贴士。

- 电脑应放在家中醒目的地方，以便成年人监督电脑的用途。
- 应在各个层面（儿童、家长和教师）进行有关计算机和如何使用互联网的教育。
- 家长和老师应在网络环境中花时间和儿童相处。
- 家长应（在与子女协商后）规定对互联网的合理用途和使用时间限制。
- 家长和教育工作者应熟悉和学习互联网上的危险。
- 家长和教育工作者应强调“不要和陌生人说话”这一原则也适用于网络环境。
- 家长和教育工作者应禁止儿童未经适当的监督就下载和/或上传图片。
- 在家庭和学校环境中都应充分利用过滤和家长控制措施。
- 家长和教育工作者有责任在儿童年幼时向他们灌输隐私的需要，并说明为什么儿童务必要尊重和寻求“不受干扰”的独处权利。

互联网协会
Galerie Jean-Malbuisson 15
CH-1204 Geneva, Switzerland
电话: +41 22 807 1444
传真: +41 22 807 1445
<http://www.internetsociety.org>

1775 Wiehle Ave. Suite 201
Reston, VA20190, USA
电话: +1 703 439 2120
传真: +1 703 326 9881
电子邮件: info@isoc.org