# 声音“窃贼”

## AI如何一秒“偷走”你的声纹？

你以为只有指纹、人脸才是身份密码？大错特错！就连你开口说的每一句话，都藏着专属的“声音身份证”——声纹。如今，这个独属我们的生物标识，只需1秒钟的语音片段，就能被AI完整复制、随意模仿。一场围绕“声音隐私”的安全保卫战，正悄然打响。

主笔：于梅君


### 1 实测惊魂：1秒复刻你的声音

当AI声音克隆的门槛低到触手可及，我们每个人的声音，都有可能成为不法分子觊觎的目标。

先看一场由央视全程记录的真实测试，结果足以让人惊出冷汗。

《法治在线》2026年4月9日聚焦AI声音克隆乱象，记者跟随网络安全专家做了一组实测：记者仅对着话筒说了一句日常话语，专家从中截取短短1秒钟的清晰音频，导入一款普通的声音克隆软件。

仅仅几秒钟，软件就生成了一段全新语音，内容是记者从未说过的话，但音色、语调、说话的气息停顿、细微语气特点，都和本人高度重合，普通人根本听不出差别。更让人警惕的是，克隆后的声音还能随意调节情绪，着急、慌张、哭腔、平缓……想切换成哪种语气都能一键调整。

1秒钟，这就是AI偷走我们声音的最短时间。不用长篇录音，不用专业设备，只要捕捉到一秒钟的有效语音，你的声音就可能被“复刻”，沦为被利用的工具。参与测试的网络安全专家直言：“现在的技术，已把声音克隆门槛降到‘人人可操作’的地步，细思极恐！”

### 2 声音“失窃”真相：你主动送出的“素材”

很多人会疑惑：我从没主动泄露过声音，AI怎么能轻易偷到？答案扎心又现实：我们每天都在不经意间，把自己的声音样本公之于众。

网络安全专家表示，只要你在微信上发过语音、在短视频平台上发布过带人声的作品、打过客服电话、使用过语音转文字功能，甚至在公共场合录音设备下说过话，就等于在网络上留下了可被采集的“声音痕迹”。这些痕迹看似不起眼，却成了不法分子获取声音素材的“宝藏库”。

也就是说，我们随手发出的一条语音、一段日常通话，都可能成为骗子伪造声音的“原材料”。不法分子无需复杂操作，只需在网络上爬取这些公开的语音片段，哪怕只有几秒，就能直接用于AI模型训练。

2025年4月，湖北黄石发生一起典型的AI语音诈骗案，被最高法列为全国警示案例。嫌疑人吴某涛，先在网络上找到一位老人孙子发布的短视频，提取其中20秒语音，通过AI克隆出一模一样的声音。

随后，吴某涛上门找到老人，当场拨通“孙子”的电话，电话里传来哭喊声：“奶奶，我打人出事了，快拿钱救我！”声音、称呼、语气都和孙子完全一致，老人毫无防备，不得不拿出养老钱“挡灾”。

不只在国内，AI语音诈骗已在全球泛滥。2026年2月，美国联邦调查局(FBI)发布警报，2025年全年AI语音克隆诈骗在美国造成的损失超8.93亿美元，约合人民币65亿元。

### 3 只需三步，AI便“学会”你的说话方式

AI到底是如何偷走我们声音的？其实，它是分三步精准复刻你的专属特征。

**第一步：提取你的“声音专属档案”。**每个人的声音，都有别人模仿不来的三大核心特征：一是音色，这是声音的“底子”，就像钢琴和吉他的音色天生不同；二是语速节奏，说话快慢、断句位置、重音落点，都是个人独有的习惯，比如有人说话尾音轻柔，有人语速急促；三是细微语气，哪怕是叹气、停顿、尾音的轻微颤抖，都是独一无二的标记。

AI不会关注你说了什么内容，只会精准抓取这些声音特征，把它们转化成数字形式，生成一份专属于你的“声音档案”。哪怕只有短短的清晰语音，AI也能提取出核心特征，完成基础档案构建。


**第二步：两个AI通过对抗式训练迭代优化，让模仿效果愈发逼真。**科学家采用简单的“对抗学习”原理，让两个AI互相配合训练：一个当模仿者，照着你的声音档案，尝试生成和你一模一样的语音；另一个当鉴定师，负责分辨这段语音是真人说的，还是AI模仿的。

一开始，模仿者生成的声音很生硬，要么语速忽快忽慢，要么没有情绪起伏，鉴定AI能轻松识别出破绽。模仿者不断纠错、优化，经过成千上万轮迭代对抗，最终鉴定师再也无法分辨真假，此时AI就彻底掌握了你的说话特点。专家比喻：“这就像教说话，孩子一开始说得乱七八糟，家长一遍遍纠正，最后孩子能说得和大人一模一样。”

**第三步：输入文字，生成你的“专属语音”。**训练完成后，不法分子输入任意文字，AI都能在半秒内，以复刻的音色、语速、语气及情绪特征生成专属语音。尤其是在实时通话诈骗中，骗子会当场播放克隆语音，与受害人直接交互，这也是AI语音诈骗屡屡得逞的原因。

### 4 防护指南：守住你的声音隐私

目前，技术公司正在研究反制手段，比如给声音添加“数字水印”或通过算法识别伪造语音，但这些技术大多尚未大规模商用，效果、稳定性与可靠性仍有待大规模实战验证。最简单、最有效的办法，是每个人都随时提高警惕。

可以设置一个“专属家庭暗号”，和家人约定一件仅属于彼此私密记忆的小事作为暗号，比如：“我小时候在姥姥家打碎的那个花瓶是什么颜色的？”AI可抓取到你所有公开的网络信息，但永远猜不到这件私密小事。

减少公开语音痕迹，不给不法分子留存可利用的语音素材。在微信、短视频平台尽量不向陌生账号发送语音；不在公开平台发布过长的语音片段，尤其是涉及个人信息、家庭情况的内容；接听陌生来电时，不透露姓名、住址、亲属关系、职业等关键信息，避免被采集更多语音样本。

网络安全专家提醒，不少人习惯在短视频中分享日常通话片段，比如“给大家听听我家孩子的笑声”“和爸妈的日常聊天”，这些内容看似温馨，实则都是完整的声音素材，很容易被不法分子截取利用。

接到陌生来电时，先沉默2秒，规避“声音采集陷阱”。骗子用于采集语音的来电，大多只有杂音、电子音，一旦发现异常，直接挂断，不闲聊、不回应。

最重要的是，无论对方是谁，无论声音多像，只要通过陌生号码、社交新号要求转账、借钱，必须挂断电话，通过通讯录中留存的亲友真实号码回拨核实，绝对不能直接转账。

最高法警示，AI声音诈骗的核心突破口就是“利用亲情、信任降低人们的防备心”，而“双重核实”是破解这一骗局的最有效手段。

**知多一点**

声纹是每个人说话时产生的声波图谱，通过专业设备可捕捉音色、音调、语速、口音、呼吸节奏等上千项细微声学特征。声纹和指纹、虹膜、人脸一样，是受法律保护的个人生物识别特征。

每个人的声纹都具有唯一性和稳定性，世界上没有两个人的声纹完全相同，哪怕是双胞胎，说话习惯、音色也存在细微差别；成年人声纹特征一旦稳定成型，便不易发生改变，具备极强的识别度。

警方常通过声纹比对技术锁定犯罪嫌疑人，比如在诈骗案件中，通过分析诈骗电话的声纹特征，排查嫌疑人身份；在金融领域，部分银行、支付平台会采用声纹验证，替代传统密码，短信验证码验证方式，提升支付安全性；安防领域，一些高端小区、办公场所会采用声纹门禁，实现无接触解锁。

《个人信息保护法》等法律法规，将声纹列为重要的个人信息，明确严禁未经本人同意，擅自收集、使用、泄露他人声纹信息。AI声音克隆的滥用，本质上就是对声纹这一生物密码的侵犯，不仅会造成财产损失，还可能引发隐私泄露、名誉损害等一系列问题。

**声纹：你的专属生物密码**

# 迷恋上AI聊天搭子？可它真的懂你吗

AI谈『心』

知心姐姐豆包

随时随地耐心倾听、永远温柔共情、秒回所有情绪……如今，越来越多人爱上AI聊天搭子，把心事、委屈、快乐悉数倾诉，甚至渐渐产生依赖，对虚拟AI萌生好感。可从心理学视角来看，这份暖心陪伴，不过是一场算法制造的情感错觉。

人类对AI产生依恋、喜爱的情绪，在心理学中被称为“情感投射效应”。

人天生有被理解、被陪伴、被无条件接纳的心理需求，当AI始终无抱怨、无指责地承接所有情绪，精准输出贴合心意的回应时，我们的大脑会自动将对真实情感联结的渴望，投射到虚拟载体上，进而误以为“AI懂我”，逐步加深情感依赖。

但要明确：AI从未拥有真正的共情力。真正的共情，是人类基于自我意识，切身感知他人情绪、并发自内心产生情感共鸣的能力，是有温度、有真实情绪体验的心理活动。

而AI的“共情回应”，只是依托大数据算法、语言模型的程序化文本输出，它没有喜怒哀乐，无法真正体会你的难过与欢喜，只是匹配了大数据中最贴合场景的“标准答案”话术。

长期过度依赖AI聊天搭子，容易陷入“虚拟社交疏离”：弱化真实社交表达能力，减少与身边人的深度沟通，看似时刻被陪伴包围，实则内心愈发孤独，慢慢丧失在现实关系里处理情绪、建立情感联结的能力。

AI聊天搭子可以是情绪的临时宣泄口，但永远替代不了家人、朋友的真实拥抱与陪伴。

分清虚拟与现实，把真心留给身边触手可及的人，才是守护心理健康的核心。

编辑：于梅君 美编：刘燕 组版：颜莉