新闻热线：010—58884062
E-mail：adaxuqian@126.com
■责编 许 茜
科技日报 2018年8月22日 星期三

想真的“美”起来，美图要从管道走向平台

行业观察

陈永伟

日前，美图创始人兼CEO吴欣鸿正式宣布该公司未来10年的战略“美和社交”，并提出了“巩固影像产品的用户优势和技术优势、用影像类APP为流量抓手，以美图秀秀和美拍为先锋产品开展社交布局”的战略。

为何一家工具提供商要将重心转到社交？笔者认为，这主要由于盈利压力。根据该公司财报，2017年美图总营收超45亿元，不过净亏损高达4600万元。

美图产品的口碑不错，但为何赚不了钱呢？原因在于其商业模式。美图的商业模式还是管道式，换言之，它主要还是通过做产品而后销售，再利用差价赚取利润。而现在成功的互联网企业大多采用平台式的模式，即通过撮合交易、促进交互来实现盈利。相比管道式，平台式可借助“跨边网络外部性”（即不同类型用户间的正向影响）实现迅速成长，也更易借力打力，其盈利机会更多、想象空间也更大。显然，美图若想突破瓶颈，必须完成平台化转型。

事实上，美图一直没有放弃过平台化的努力，并且曾有过两次很接近成功的经历。

一次是用美拍进军短视频市场。这款以女性为目标用户的APP在2014年5月上线后，曾连续24天蝉联App Store免费总榜冠军，其市场认可度可谓不低。不过，这款开局不错的APP未能抓住短视频的风口。既没有赶上前辈快手，也没有赢过新秀抖音。

另一次是用闪聊进军即时通讯领域。闪聊于2016年10月发布后，曾以其新奇的社交方式、符合年轻人交流习惯等特点迅速在90后、00后中扩散。不过，它同样没有延续开局的幸运，不久后就出现了疲软，不到两年就停止了运营。

总的来说，这两次失败还是源于战略失误。无论是短视频还是即时通讯，美图都是后来者，市场上已有强大的在位者。面对这种情况，美图选择了在开始时深耕利基市场，即那些被市场中的统治者或优势企业忽略的、新兴或未被发现的细分市场。这个选择是对的，它也确实借此很快发展起了自己的“种子用户”。不过，在这之后，美图的出招就有失水准了。

考察一下成功社交平台的成长经历就不难看到，其成长一定会经过一个突破原有用户群的过程——起家于年轻人的QQ如此，起家于校园用户的脸书更是如此。只有这样，才能最大限度地激活平台的“跨边网络外部性”，使其迅速成长。而美图显然没有认识到这一点，而止步于女性市场和年轻人市场。这导致平台用户过于同质化，无法发挥“跨边网络外部性”的作用，而只能借助“同边网络外部性”来吸引用户，因此其成长速度就会非常缓慢。

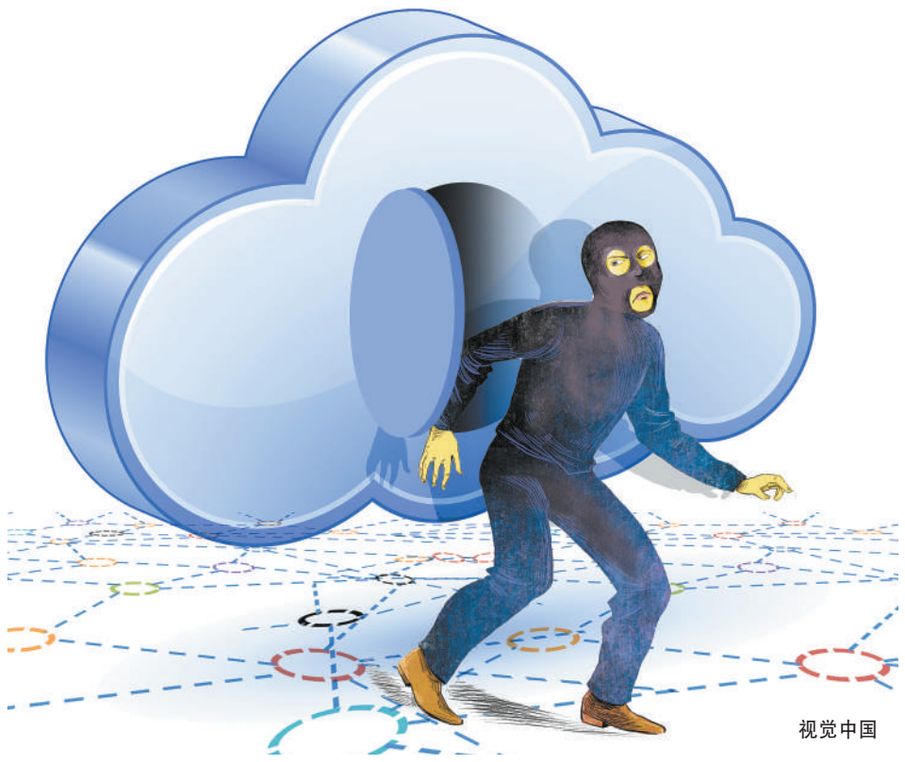
当然，现在美图手里的牌还有不少。美图秀秀具有巨大的流量潜力，而美拍上的大量“白富美”用户更是优质资源。不过，究竟美图能否打好这些牌、完成逆袭，恐怕还需要时间来检验。

腾讯云丢数据 云安全遭拷问

本报记者 刘园园

声称云服务器数据可靠性达99.9999999%的腾讯云，却把数据弄丢了。

近日，创业公司“前沿数控”怒怼腾讯云，称其放在腾讯云服务器上的数据全部丢失，给其公司业务带来灾难性损失。腾讯云随后对这一事故予以承认并表达歉意。目前，双方已制定出共同认可的业务解决方案。虽然事件暂告一段落，但此事还是引发了公众对云服务安全的关注。


视觉中国

事因“屋漏偏逢连夜雨”

被怒怼后，腾讯云公开了此次故障的来龙去脉。

腾讯云在其官方微信公号发布《关于客户“前沿数控”数据完整性受损的技术复盘》，其在该文中解释说，当天运维人员收到仓库Ⅰ空间使用率过高告警，从仓库Ⅰ选择一批云盘搬迁至新仓库Ⅱ。为加速搬迁，手动关闭了迁移过程中的数据校验。

搬迁完成后，为了释放空间，运维人员对仓库Ⅰ中的源数据发起回收操作。当天晚上监控发现仓库Ⅱ部分云盘出现异常。

“该故障缘起于因磁盘静默错误导致的单副本数据错误，再加上数据迁移过程中的两次不规范操作，导致云盘的三副本安全机制失效，并最终导致客户数据完整性受损。”腾讯云总结说。

北京理工大学网络攻防对抗技术研究所所长闫怀志用“屋漏偏逢连夜雨”来形容这次事故。

首先，腾讯云提供的云盘因所在物理硬盘固件漏洞导致静默错误。闫怀志解释说，硬盘存储硬件并非完美，因此设计了硬盘出错及异常报警机制。但该机制并不能将漏洞与错误全部识别并进行正确处理，偶尔会出现“漏网之鱼”，而且只有在用户使用的时候才会暴露出来，也就是出现静默错误。

“静默错误一旦发生在元数据（用来描述数据特征的系统数据）中，将造成不可挽回的数据损失。”闫怀志对科技日报记者说。

但他认为，更重要原因是云服务提供商违反了基本的数据迁移操作规范。因为正常的数据迁移默认使用数据校验功能，此外，还需对源数据仓库进行一定期限的数据保全，待确认迁移数据无异常后，方可进行仓库回收。

而运维人员的操作连续违反上述操作规范，致使数据迁移出现异常后，又提前对源数据进行仓库回收。通常云服务商会采取对数据进行3个备份的机制来保障数据安全性，但两次违规操作，使数据异常扩散至三副本，最终导致数据无法恢复。

三分靠技术七分靠管理

云服务到底安不安全？所谓的数据可靠性达99.9999999%，夸张吗？

“这些年与数据安全相关的技术一直在不停迭代、升级，可以说已非常成熟。”华云数据执行副总裁、首席技术官谭瑞忠在接受科技日报记者采访时表示。

谭瑞忠认为，腾讯云声称云服务器数据可靠性达99.9999999%，是单纯从技术角度计算出来的，并没有夸大。但很多时候存储在云端的数据丢失、被破坏或被盗取不是因为数据安全技术不可靠，而是人为原因。

拿此次腾讯云事故来说，谭瑞忠认为，假如只是磁盘静默错误导致迁移数据时出错，而并没有后续的运维人员违规操作，“前沿数控”的数据完全可以通过数据三副本机制找回。

“木桶理论警告我们，无论是技术短板还是管理短板，都会拉低云计算的整体安全性。”闫怀志说，这次事故再次证明信息安全三分靠技术，七分靠管理。

闫怀志认为，企业不能天真地将云计算视作万能良方，认为将数据上云就能保障安全、一劳永逸，因为绝对的安全是不存在的。

在闫怀志看来，从根本上来说，云服务安全保障没有什么捷径可走，应从技术和管理两方面入手，完善云存储信息安全保障体系。比如，在技术上，可以强制进行数据安全全流程校验，提升数据运维的流程化、规范化、自动化水平，减少甚至避免人工干预。在管理上，不仅应制定更为完善的管理体系，更应注重管理制度及措施的落实。

“从行业发展趋势来看，云服务商都在努力将人工干预降到最低，提高云服务运营的自动化。”不过，谭瑞忠还建议，应推动云服务的开放性，也就是让用户的数据可以在公有云、私有云等不同云环境甚至不同云服务商之间自由迁移，并实现数据的实时同步，这样相当于给用户数据上了“双保险”。

数据价值界定仍是难题

此次腾讯云事故引起关注的另一个细节在于，腾讯云与“前沿数控”曾就赔偿问题产生较大分歧。

据报道，“前沿数控”向腾讯云提出了1100万元的赔偿要求，而腾讯云则给出了“赔偿+补偿”总金额为13万余元的解决方案。

“由于数据具有虚拟性和实质性的双重属性，数据价值的界定一直是老大难问题，在数据损失赔偿方面也容易产生分歧。”闫怀志说。

“数据对企业生存越来越重要。”谭瑞忠告诉科技日报记者，但目前对数据价值的评估确实还没有成熟的方法。他认为，在出现类似事故后对数据价值的判断可以从多个维度来考虑。

谭瑞忠解释说，判断数据价值的维度应该包括：客户业务对数据的依赖性，这需要对客户公司运营的方方面面进行深入了解；数据的破坏量，比如若只丢失了30分钟的数据，则只考虑30分钟数据的影响；云服务提供商与客户分别承担的责任等。就此次事件，谭瑞忠认为，除了将责任归咎于云服务商，也应考虑到客户并未对数据采取保护措施的责任。

闫怀志也认为，云安全的责任问题牵涉到云服务提供商和客户两方面。针对本次事故而言，云服务提供商应负主要责任，而客户也该采取必要的备份措施以防万一，比如开启快照功能对重要数据定期备份等，绝不能做“甩手掌柜”。

在数据价值界定问题上，闫怀志认为，云服务商在为用户提供云服务时，可提前进行安全风险评估，协商确认数据价值。用户如果声称自己的数据价值高，云服务提供商就可据此要求收取相应较高的服务费用，做到责权利平衡。在发生事故进行赔偿时，也有参考标准。

“另外还可考虑设立数据第三方保险索赔制度。”闫怀志说，也就是为需要保护的数据投保并缴纳相应保费，一旦出现数据受损的情况，可根据投保额进行索赔，这样就转移了云计算服务提供商和用户的损失风险。

热点追踪

暗网惊现美军涉密资料——

黑客如何潜入固若金汤的军方网络

实习记者 于紫月

据外媒报道，近日有黑客在暗网售卖美国MQ—9无人侦察机、M1主战坦克等的相关涉密资料。上述报道中称，该黑客利用Netgear路由器漏洞入侵美国军方网络，窃取了这些涉密资料。

黑客如何潜入固若金汤的军方网络？对此，恒安嘉新（北京）科技股份公司安全研究中心网络安全专家周忠义分析称，黑客有可能采用了如下攻击方式：首先用搜索引擎Shodan找到含有漏洞的Netgear路由器；而后用FTP弱口令登录路由器，再通过路由器上的漏洞获取访问权限，进而植入木马。随后，他们对网络流量进行监控、过滤，并从美国军方网络终端窃取了机密文件。

“这套攻击手段的技术含量很高。”周忠义认为，美军方网络不可能“弱不禁风”，虽然存在弱口令这样的低级失误，但这并不能直接导致数据泄露，所以黑客极有可能掌握了高水平的“零日漏洞”（zero-day）攻击方法，最终实现了信息窃取。

资料显示，“零日漏洞”又被称为零时差攻击，是指被发现后立即被恶意利用的安全漏洞。

那么，黑客为何选择在暗网进行资料交易？

所谓暗网，就是指那些存储在网络数据库里、但不能通过超链接方式访问而需通过动态网页技术访问的资源集合。传统的搜索引擎“看”不到、也“抓”不到这些存储于暗网的内容，除非通过特定的搜索技术才会看到这些页面。

周忠义告诉科技日报记者，正是由于暗网具有难追查的特性，使其成为网络不法交易的“天堂”。暗网被部署于匿名网络之中，访问者和被访问者都被隐藏起来。而匿名网络由全球的动态网络节点组成，跨越不同国家与地区，加之通信加密，难以实施监听与定位。

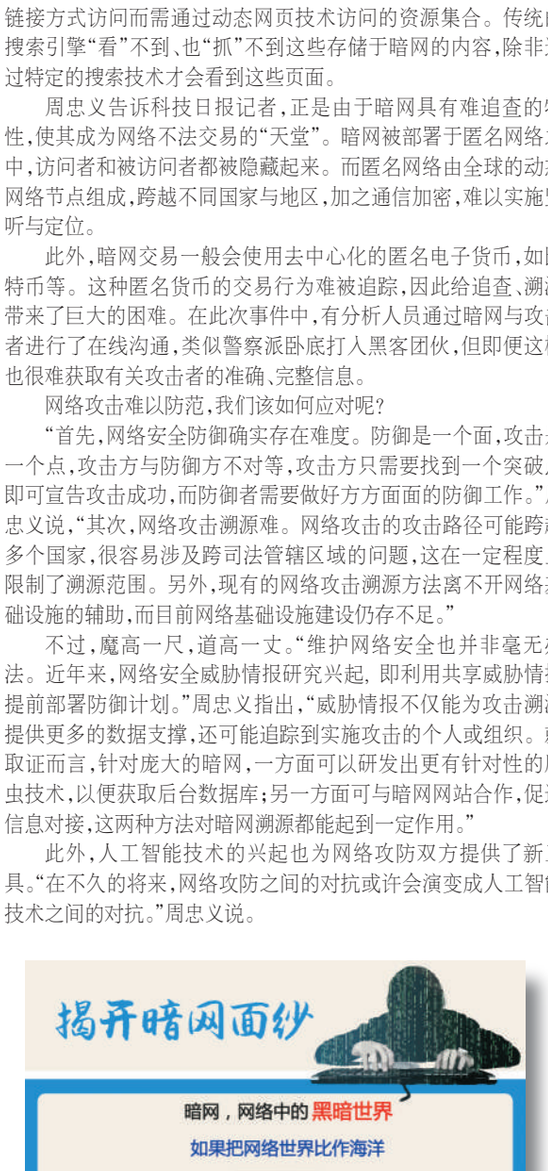
此外，暗网交易一般会使用去中心化的匿名电子货币，如比特币等。这种匿名货币的交易行为难被追踪，因此给追查、溯源带来了巨大的困难。在此次事件中，有分析人员通过暗网与攻击者进行了在线沟通，类似警察派卧底打入黑客团伙，但即便这样也很难获取有关攻击者的准确、完整信息。

网络攻击难以防范，我们该如何应对呢？

“首先，网络安全防御确实存在难度。防御是一个面，攻击是一个点，攻击方与防御方不对等，攻击方只需要找到一个突破点即可宣告攻击成功，而防御者需要做好方方面面的防御工作。”周忠义说，“其次，网络攻击溯源难。网络攻击的攻击路径可能跨越多个国家，很容易涉及跨司法管辖区域的问题，这在一定程度上限制了溯源范围。另外，现有的网络攻击溯源方法离不开网络基础设施的辅助，而目前网络基础设施建设仍存不足。”

不过，魔高一尺，道高一丈。“维护网络安全也并非毫无办法。近年来，网络安全威胁情报研究兴起，即利用共享威胁情报提前部署防御计划。”周忠义指出，“威胁情报不仅能为攻击溯源提供更多的数据支撑，还可能追踪到实施攻击的个人或组织。就取证而言，针对庞大的暗网，一方面可以研发出更有针对性的爬虫技术，以便获取后台数据库；另一方面可与暗网网站合作，促进信息对接，这两种方法对暗网溯源都能起到一定作用。”

此外，人工智能技术的兴起也为网络攻防双方提供了新工具。“在不久的将来，网络攻防之间的对抗或许会演变成人工智能技术之间的对抗。”周忠义说。



分发盗版内容，这家公司和腾讯成被告

第二看台

本报记者 张盖伦

前不久，维权骑士向杭州互联网法院提起诉讼，把腾讯和一家小程序开发企业一块给告了。

维权骑士是国内70余家内容企业的版权管理与保护体系解决方案提供方，他们的日常工作之一，就是和各种盗版行为斗智斗勇。

这次主要的被告方是长沙百赞网络科技有限公司（以下简称百赞），其旗下有多个小程序和微信公众号。这些小程序不生产知识，只是知识的“搬运工”。它们侵权了多家平台上的知识付费产品，并靠着这些产品，为公众号引流涨粉。

被告二则是腾讯。“我们希望微信重视平台上的盗版行为，切断未经许可传播付费作品的途径并给予有效的处罚。”维权骑士副总裁宏达这样解释他们的诉讼初衷。

通过“群裂变”为公号涨粉

《武志红的心理学课》，在知识付费平台得到APP上的定价是199元，近20万人正在学习。

但在其他平台上，同样活跃着这门课的听众，他们不用花钱。想要免费课程很简单，你只需进入某个微信群，关注公众号或小程序，用自己的朋友圈打个广告，发一张“扫码获得XX课”的图片就行。

此时，你将自己变成了“群裂变”中的一个传播节点，你的报酬就是免费的知识付费产品。

靠着一条条朋友圈、一个个二维码，公号运营者可以在短期内建起大量微信群，并为自己的公号引流。

得到是维权骑士的客户之一。版权维护人员为了搜集侵权证据，“卧底”过不少这样的群。

“微信平台对于该类行为，仅能以‘诱导分享’进行投诉，没有盗版侵权相关投诉选项。”宏达说，“就算以诱导分享举报成功，平台也仅是限制二维码指向链接在朋友圈的传播，但图片不做任何处理；通过识别二维码，也依然能正常跳转到二维码的指向链接。”虽然也有过投诉成功的经历，但他们也知道，这批人就算放弃了一个公号，也可以迅速另起炉灶，同样的生意在短时间内又能做起来。

让人感到棘手的是，和群裂变关联的公众号大多是个人号，可以轻易通过公众号迁移的功能卖给其他人。“这些号频繁过户，侵权权利人难以明确，证据灭失也很快。”宏达认为，“要有效处理这类问题，平台必须有所作为。”

想用诉讼给业界提个醒

对这些有前科的公众号，不管他们转了几次手，维权骑士也依然在持续监控。

近期他们发现，其中一些公众号关联上了小程序，以小程序作为盗版内容传播载体。

百赞旗下的众多小程序，就是一个盗版内容“集中营”。以小程序“回播”为例，进入首页，你就能看到许多其他平台的热门付费内容：《蒋勋细说红楼梦》，显示有191万人收听，这本为蜻蜓FM的付费内容；《DR魏的家庭教育》，显示6.1万余人收听，为“得到”APP的付费内容……只要你按照提示，将内容分享到朋友圈或微信群，就能免费收听。

百赞运营了多个小程序，小程序下又关联了多个微信公众号。侵权还形成了“矩阵”，这让维权骑士感到哭笑不得。但好处是，他们可以确认小程序开发公司的主体。

于是，维权骑士向百赞提起了诉讼，请求法院判令其停止侵权，要求其赔偿经济损失及合理费用共计人民币5万元。

而被告二，就是腾讯。

宏达解释，团队此前曾与微信平台进行过多次沟通，但他们未有效遏止盗版行为。“微信体系内，盗版产业规模不小。我们挑选这个案例，希望能以典型案例来警醒平台和业界，我们对于版权保护这件事，是严肃且认真的。”

中国政法大学知识产权研究中心特约研究员李俊慧曾在接受科技日报记者采访时表示，小程序主要依托微信平台生存，微信平台对于小程序的上架、下架以及投诉处理，都应该建立完善的机制。比如畅通投诉举报机制、事前著作权归属核验机制、事中纠纷调解机制等。而如果判定侵权，也要对构成侵权的产品及时予以下架。

目前，根据杭州互联网法院诉讼平台上显示的信息，该案已立案成功。截至8月21日记者发稿，两方被告都没有主动联系维权骑士。

“我们的态度也很坚决，侵权问题必须得到有效遏制。平台方要承担责任，不管对方是不是腾讯。”宏达说，他们希望借由诉讼提醒小程序开发者要遵守法律、法规，希望监管、司法部门加大对这种新业态的关注。“微信目前对著作权的关注度太低，相关问题处理的规则不明、惩罚不严、渠道不通。我们也希望通过案例敦促他们更加重视著作权保护。”宏达强调。