经济参考报/2012 年/3 月/20 日/第 008 版
思想 · 法眼

网站用户密码泄露的法律对策

中国社科院法学所　沈卫利

去年十二月，国内知名的程序员网站、IT 技术社区 C SD N 的 600 多万个注册邮箱账号和密码数据库被黑客在网上曝光，并引发一系列的连锁影响。联系近年国内外的许多网站信息泄露事件，网络信息安全问题成为我们必须思考和重视的话题。

国内外的“ 泄密门 ”成为严重挑战

此次密码泄露事件中，有一点可怕的是，这些用户密码是以明文方式保存的，即网站方面未采取任何加密安全措施，从而使这些被曝光的用户密码数据库在网上被公开传播。虽然过去也有类似事件，但此次流传的范围超出了以往的黑客技术圈界限，普通用户也可通过数据包下载方式获得网站泄露的用户资料和密码。这无疑突破了用户密码这一个人数据与隐私的最基础防线，让心怀不轨之不法之徒有可能窃取他人的个人数据。

而按照许多用户的注册密码使用习惯(特别是早期上网的老用户)，他们用一个注册账号(电子邮箱地址或个人 ID)登录多家网站，包括门户网站、电子邮件服务、网络银行、社交网站、游戏网站等，并在多家网站同时使用相同密码。这种做法虽然简单省事，易于操作，但是在网络安全泄密事件频发的今天，其风险程度令人堪忧。按窃密者操作路径，他们会用这些公开密码进入他人邮箱或其他网络账户，并举一反三，在获取用户多账户信息的同时进一步获得用户的联系人信息，然后将这些信息转让、出售或直接用其谋取利益。

CSD N 网站用户信息被泄引发了国内多家网站的连锁反应，许多著名门户网站和商业网站未能幸免。不仅如此，一些政务网站也身陷“ 泄密门 ”。不久前，有网友通过新浪微博发帖称，广东省公安厅出入境政务服务网后台存在漏洞，造成大范围用户数据泄露，暴露的用户申请资料高达 440 多万条，这些记录包括用户的出身年月、邮寄地址、邮编、电话、通行证件有效期、出境事由等详细信息。

前段时间集中爆发的网站密码泄密事件并非偶然，去年四月下旬，电子游戏巨头日本索尼公司的 PS3、PSP 网络平台 PSN 因受到黑客攻击而停止服务。事后索尼发出正式公告，约 7700 万用户个人数据被盗，包括用户 ID、住址、电子邮箱地址、出生日期、密码、登录日志、信用卡号码等。事发后，索尼向用户支付了 7000 万美元的赔偿金，但索尼对黑客的真实目的和攻击策略仍不甚了了。

由于黑客攻击导致用户个人数据大规模泄露，曾力主实行网络实名制的韩国不得不提出分阶段逐步废止网络用户实名制。此前，韩国三大门户网站之一的 N ate 和社交网站赛我网分别外泄了 3500 万多名用户的个人数据。这起韩国历史上影响最大的网络安全事件所泄露的用户信息非常详尽，包括用户名、本人姓名、生日、电话号码、住址、网站密码和身份证号码，范围之广，几乎涉及韩国所有网民，并很有可能引发垃圾电邮和电信诈骗等衍生犯罪活动。

信息技术的高速发展和互联网的迅速普及给网络安全带来了日益严重的挑战，也对信息安全相关法律及其监管提出了新的课题。

网站信息安全的法定等级较低

网络用户的密码其实是一种口令(Passw ord)，它与用户其他个人信息组合成为个人数据，它不是专业意义上的密码。但它的认证、保管与使用也需要相应的密码技术与密码产品(如网络银行使用的 U 盾)。所以二者是密不可分的。

目前我国关于信息系统安全的相关法律和法规有：《中华人民共和国计算机信息系统安全保

护条例》、《商用密码管理条例》、《信息安全等级保护管理办法》，以及修改后的刑法与其他法规的相应条款。其中，《商用密码管理条例》规定了商用密码的科研、生产、管理和销售具体办法，其中第二十三规定：泄露商用密码技术秘密、非法攻击商用密码或者利用商用密码从事危害国家的安全和利益的活动，情节严重，构成犯罪的，依法追究刑事责任。

2007 年，公安部、国家密码管理局、国家保密局和国务院信息办公布了《信息安全等级保护管理办法》(以下简称办法)，该办法对信息安全保护的基本思路是：国家通过统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级地实行安全保护，并对等级保护工作的实施进行监督、管理。

信息系统的安全保护等级的确定依据主要有两条：一是根据它在国家安全、经济建设、社会生活中的重要程度；二是系统一旦遭到破坏，它对国家安全、社会秩序、公共利益以及公民、法人和其他组织合法权益的危害程度。据此，办法将我国信息系统共分为五个等级。第一级是指信息系统被破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。第二级指信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。第三级、第四级分别指信息系统受破坏后，会对社会秩序和公共利益造成严重损害，或对国家安全造成损害；会对社会秩序和公共利益造成特别严重损害，或对国家安全造成严重损害。等级最高的第五级是信息系统受破坏后，会对国家安全造成特别严重损害。

近年来，由于智能手机、移动互联网、社交网络、微博、即时通讯软件等新技术的突飞猛进，互联网已成为一个跨平台的超级信息系统。然而，按照传统的等级保护管理规定，国内许多内容服务商、门户网站、社区网站、游戏网站最多属于第一级或第二级保护范围，而对这两级监管的法律规定是“ 依据国家有关管理规范和技术标准进行保护，国家信息安全监管部门对其安全等级保护工作进行指导。” 其保护等级明显低于第三、四、五级。

网站的安全投入严重不足

技术发展在给人们带来便利的同时也带来了潜在的危险。今天，黑客和其他网络犯罪行为的门槛越来越低了，并不需要高深的计算机专业知识。有时，一个菜鸟级新手，只要稍加搜索和学习，就能从网上方便地获得大量资源和工具，同时还能轻而易举地找到同道和犯罪同伙。黑客的组织化、社区化、匿名化和国际化已经成为新趋势。这些人通过社区、Q Q 群和各种即时通讯工具在第一时间互相切磋，破解用户密码并盗取资料，且用户数据买卖销售已成为相当具有规模的固定产业链。虽然黑客社区联系松散，甚至彼此从未谋面，尚不知对方是男是女，但利益链条将他们捆绑在一起。与商业网站的被动安全措施相比，由于利益驱动和贪欲渴望，这些人无时无刻地在寻找网站的安全漏洞，期待从中找出发财机会。

相比之下，商业网站、各种社交网站的安全维护并不能给网站带来直接经济利益。许多网络服务商、内容提供商对安全的投入严重不足，从笔者接触的研究资料看，除排名前百名的大型网站外，国内鲜见有专门安全团队的商业网站。政府的政务网站也存在大量安全漏洞，一些政府网站被轻易篡改或挂马。据国家互联网应急中心监测报告显示，2011 年 6 月的某一周，国内仅网页被篡改的网站就有 660 个，其中政府网站 105 个。其中包括 6 个省部级网站，还有 25 个地市级政府网站。

为应对网络安全的挑战，可以从完善法律体系和行政监管、行业组织协调和网站加强自律责任等方面入手，当然用户也需要提高风险防范意识。

政府要完善法律体系和行政监管

几年前，国务院信息产业主管部门曾起草过《信息安全条例》，但迄今未有下文。面对日益严重的网络安全威胁，应当有一部层级较高、操作性强的信息安全综合法规，以便为信息安全的法律监管提供法律依据，同时，应强调行业组织的自律与企业自律，鼓励企业提升安全保护措施。

对个人数据的保护，国外有代表性的保护模式是欧盟与美国。欧盟有统一的个人数据保护法，

在电子商务、电子政务方面拥有大量标准规范，欧盟各成员国必须遵守。美国模式则强调发挥商业企业的创新精神，但政府也不是无为而治。上个月，奥巴马行政当局就提出了网络隐私保护准则，旨在帮助消费者控制网络搜索对个人隐私的损害。新的隐私保护法律要求网络企业必须为用户提供一健式点击或触摸的告知程序，让用户决定他们是否愿意自己的个人数据被追踪。美国国会也将起草有关个人数据搜集和使用的监控法案，一旦通过，谷歌、微软、苹果和其他浏览器制造商都必须遵守相关法律。

网站不能推卸自己的法律责任

从发生泄密的源头看，近来几大事件均发源于网站服务端。对此，处于客户端的用户是心有余而力不可及。因为用户一旦与网站签约(成为网站用户，无论是否活跃)，他的个人数据就处于本人不可控的状态。因此，网站的个人数据保护责任是不可推卸的。

按照《侵权责任法》法定侵权要件和合同法的契约精神，无论是作为企业还是作为合同签约一方，网络服务商都有责任保护用户数据安全。但许多企业不是视而不见，就是在格式合同中用含糊其辞的条款弱化自己责任，这极不公平，更违反了网络企业的法定义务。

在保护用户个人数据方面，网络服务商、运营商应当恪守以下义务：

一、个人数据安全风险提示义务：服务商应当向用户说明提交个人数据的潜在风险，并做出保护个人数据的安全承诺。

二、个人数据用途说明义务：网站应说明用户数据的具体用途，说明这些数据是否与第三方分享，或是否可能向第三方转让。

三、保护用户个人数据安全的义务。

四、安全措施说明义务。

五、发生数据泄漏后的告知、救济义务。如即时通知用户修改密码，损害实际发生后的补救措施等相关善后事务。

网民自身也要有所作为

普通网民也需要提高风险风范意识，网民自身需要做好下列事项：

用户应当对自己的密码进行分类保管。在预见损害后果的基础上按照风险等级将密码分类，比如网络银行密码、支付网站密码、电子邮件密码、即时通讯密码、社区网站密码等。如实在有困难，可退而求其次，将网络银行和支付工具密码列为首位，将娱乐网站和社交网站放在较次要地位。

密码应尽量使用数字与字母组合，并力求避免生日密码或普通排列数字密码。

有些网民从不用网银，也不用支付工具，他们觉得这样就可以高枕无忧了，其实并不尽然。黑客可能用批量扫描方式获取邮箱密码和你的联系人信息，下一步，无孔不入的营销公司和诈骗团伙会盯上你的社交圈子和朋友。

网络信息安全是一场永远不会完结的猫捉老鼠游戏，我们每个人都置身其中，无法逃避。