第1章

隐私泄露案例与现状分析

1.1 概述

随着信息网络和基于信息网络的各种应用的不断发展和普及，大量的个人隐私数据存在于网络空间。隐私泄露事件不断发生，泄露的内容五花八门，包括个人终端文件、个人身份信息、网络访问习惯、兴趣爱好乃至邮件内容等，隐私泄露问题已成为人们广泛关注的焦点。隐私数据泄露不仅会影响到个人利益，甚至威胁到国家的网络空间安全。

隐私数据的来源主要包括主机设备（如个人终端设备、服务器等）以及网络空间。其主要获取手段除了通常的恶意软件、网络数据包截获外，还包括通过应用软件对用户行为信息的采集等。近年来，国内外数据隐私泄露事件频发，令人触目惊心。早在2010年，奇虎360公司和腾讯公司之间就爆发了著名的“3Q”大战，至今令人记忆犹新。两家公司相互指责对方的软件泄露了用户的隐私，继而引发了中国互联网历史上第一次因为隐私泄露问题而波及近八成网民的重大事件。此后涉及隐私泄露的事件层出不穷，例如国内2011年发生的CSDN用户账号密码泄露事件，国外2010年发生的谷歌街景图片侵犯个人隐私事件等等。据媒体调查显示，55.8%的受访者认为保护个人隐私越来越难，29.3%的受访者认为个人信息被随意公开泄露。据美国媒体报道，2013年3月11日，美国18位政要和名流的隐私信息被黑客在网络上曝光，受害人包括美国第一夫人米歇尔、副总统拜登、联邦调查局局长穆勒、碧昂斯夫妇等，公开的信息包括住址、电话号码、身份证号码、住房按揭账号、信用报告等。试想这些政要和名流的隐私信息如果涉及国家安全和政府机密，造成的后果将不堪设想。

另一方面，美国等国家也一直在采用各种手段监视和采集用户的隐私数据。2013年爆发的斯诺登事件，使人们对大规模元数据采集后的元数据的价值与地位有了全新理解，对元数据所涉及的个人隐私等问题有了全新的认识与定位。同时，美国利用自

身在 Internet 物理拓扑上的中心地位的优势，截获互联网中转数据，甚至入侵他国网络核心设备，更改路由配置，盗取数据。没有规范的数据采集法律法规和有效的数据隐私泄露行为的分析技术，就难以保障用户隐私数据不被窃取和非法使用。但从长远看，网络空间隐私保护治理是一个趋势，网络安全国际合作也是必然。如此众多的实例表明，隐私泄露问题极大地影响了人们正常的网络生活，对于互联网的健康发展极为不利，已成为亟需解决的互联网安全问题，对隐私泄露问题的分析和研究已成为具有重要意义的研究方向。

1.2 隐私

1.2.1 定义和分类

隐私一词，顾名思义是隐秘的、私人的事情，源于人类天生的羞耻感。隐私的概念古已有之，我国周代的诗经《小雅·大田》便有诸如“雨我公田，遂及我私”的诗句。然而由于隐私一词含义的模糊性和多样性，人们仍然很难给出其完备的定义。广义上来说，隐私描述的是保持独立不受侵扰的权利。隐私涉及的主要类型包括基本人身隐私、个人相关信息的隐私、个人精神和情感的隐私、组织相关信息事务的隐私等诸多方面，其中：①基本人身隐私最为直白，通常是具体可见的事物，包括人体的私密部位、个人的独立空间、个人的财物等；②个人相关信息的隐私是指能够和个人关联起来并识别个人身份，但是当事人不愿意被他人知晓的信息，此类隐私包含的内容极为宽泛，大致分为个人日常活动、个人经历、个人财务状况、个人健康状况等；③个人精神和情感的隐私主要指精神领域的个人隐私，包括宗教信仰、性取向、政治立场等；④组织相关的信息和事务的隐私主要指政府机关、公司、社会团体和其他组织的重要信息和商业机密等，虽然不涉及某个个人，但同样也属于隐私的范畴。由此可见，隐私涵盖了个人及个人生活的几乎所有环节，同时也涉及社会生活的大多数领域。

有关隐私的首次正式书面定义发表于 1890 年的《哈佛法律评论》，Samuel Warren 和 Louis Brandeis 等人称：“Privacy is the right to be let alone”。1995 年 10 月美国商务部电信与信息管理局发布的关于隐私与信息高速公路建设的白皮书曾经给出了更为具体的解释，“隐私”至少包括以下 9 个方面的内容：①关于私有财产的隐私；②关于姓名与形象利益的隐私；③关于自己之事不为他人干涉之隐私；④关于一个组织或事业内部事务的隐私；⑤关于某些场合不便露面的隐私；⑥关于尊重他人不透露其个人信息之隐私；⑦关于性生活及其他私生活之隐私；⑧关于不被他人监视之要求的隐私；⑨私人相对于官员的隐私。美国 1974 年制定《联邦隐私权法》，1986 年通过《联邦电子通信隐私法案》，2000 年 4 月出台了第一部关于网上隐私的联邦法律《儿童网上隐

私保护法》，还有《公民网络隐私权保护暂行条例》、《个人隐私权与国家信息基础设施》等作为业界自律的辅助手段。

欧盟在1997年通过《电信事业个人数据处理及隐私保护指令》之后，又先后制定了《Internet上个人隐私权保护的一般原则》、《信息公路上个人数据收集、处理过程中个人权利保护指南》等相关法律。

在中国现行法律中，最高人民法院2001年3月公布的司法解释中明确了对隐私权的保护，强调“侵害他人隐私”即是违反法律和公共道德。《侵权责任法》第二条给出的民事权益范围中包括了对于侵犯隐私权的定义，包括：①未经公民许可，公开其姓名、肖像、住址和电话号码；②非法侵入、搜查他人住宅，或以其他方式破坏他人居住安宁；③非法跟踪他人，监视他人住所，安装窃听设备，私拍他人私生活镜头，窥探他人室内情况；④非法刺探他人财产状况或未经本人允许公布其财产状况；⑤私拆他人信件，偷看他人日记，刺探他人私人文件内容，以及将其公开；⑥调查、刺探他人社会关系并非法公之于众；⑦干扰他人夫妻性生活或对其进行调查、公布；⑧将他人婚外性生活向社会公布；⑨泄露公民的个人材料或公诸于众或扩大公开范围；⑩收集公民不愿向社会公开的纯属个人的情况，等等。

1.2.2　隐私数据

现阶段随着互联网的发展，信息的流通变得高度发达和便捷，传统的隐私内容都可以以信息的形式被互联网收集、传输和存储，这类隐私相关的数据构成了新的隐私形式——隐私数据。隐私数据有多种承载形式，包括：

(1) 个人本地数据资料。用户的个人文档、照片、视音频、日记、通讯录等等，作为最为基本和私密的个人隐私数据存储于个人计算机上。

(2) 网站登录的个人身份信息。网络用户在申请上网开户、个人主页、免费邮箱以及申请服务商提供的其他服务(购物、游戏、医疗、交友等)时，服务商往往要求用户提供姓名、年龄、身份证号、工作单位、住址等信息，这些用户信息均属于个人隐私数据。

(3) 个人的信用和财产状况，包括信用卡、电子消费卡、上网卡、上网账号和密码、交易账号和密码等。个人在上网、网上购物、消费、交易时，登录和使用的各种信用卡、账号均属重要的个人隐私数据。

(4) 电子邮件地址。邮箱地址同样也是个人的隐私，用户大多数不愿将之公开。掌握、搜集用户的邮箱，并将其公开或提供给他人，致使用户收到大量的广告邮件、垃圾邮件或遭受攻击，使用户受到干扰，显然也侵犯了用户的隐私权。

(5) 网络通信内容。各类通信软件和聊天平台收集并存储了大量的文字和视音频通信内容，直接涉及通信参与者的个人隐私。此类隐私事关当事人的私密交流和情感问题，往往容易引发严重的后果。

(6) 社会关系。随着社交网络的快速发展,人们在网络上的社交关系越发紧密和复杂,甚至与实际的社交关系息息相关。通常人们只愿意与自己的好友分享这些社会关系,因此,此类信息也成为用户的重要隐私,对这种隐私的保护可以使人们在网络上保持虚拟身份和生活中的真实社交关系不受侵犯。

(7) 网络活动踪迹。个人在网上的活动踪迹,如 IP 地址、浏览踪迹、活动内容,均属个人隐私。显示、跟踪并将该信息公之于众或提供给他人使用,也属于侵权。比如,将某人的 IP 地址告诉黑客,使其受到攻击;或将某人浏览黄色网页、办公时间上网等信息公之于众,使其形象受损,这些也可构成对网络隐私权的侵犯。

(8) 个人习惯爱好。人们在参与网络活动时往往会暴露自己的个性与爱好,这些信息在某些场合具有一定的商业价值,因此可能被分析和利用。以网络购物为例,用户的浏览历史往往体现用户的购物习惯和主要爱好,这些信息有可能被服务商用来分析并提供定向的广告,但这往往是用户不希望看到的,因此也构成了对于用户隐私的侵犯。

(9) 位置信息。在智能手机、平板电脑和车载设备等移动终端普及的今天,位置信息成为一项新的个人隐私。这种隐私能够精确地反映人们的日常活动轨迹,在很多场合很容易暴露用户的隐私。在许多移动终端应用中,都能够轻易地获取并分发位置信息,如果没有合适的控制和约束,将会使用户陷入窘境。

互联网时代的隐私数据越来越多地引起人们的关注,各种隐私泄露事件的起因往往都是某种不应被公开的个人隐私数据泄露到了互联网上,导致个人的权利受到侵害。因此,本书所讨论的隐私就是隐私数据,具体是指所有涉及个人隐私的数据。用户的隐私数据在被收集、存储和传输的过程中被未经许可的第三方实体获得的行为称为隐私泄露行为。

1.2.3 隐私数据泄露途径

互联网上隐私数据的泄露主要发生在 3 个层面:主机层面、数据传输层面和网络服务层面。*主机层面*的隐私泄露最为广泛和严重,用户日常使用计算机的过程会在个人主机上产生大量的隐私数据,很容易被同时运行于用户主机之上并以泄露用户隐私为目的的软件窃取。*数据传输层面*的隐私泄露是指隐私数据在网络传输过程中被监听和截取,这也是攻击者常用的手段和隐私泄露的重要方式之一。*网络服务层面*的隐私则是一种较为新兴的泄露方式,在各种网络服务中,如网络社区、社交网络、微博等等,参与的用户往往会在网站上保留一定的个人信息。如果服务设计存在缺陷或者用户数据库被直接攻陷,大量的相关用户隐私则会发生泄漏。

由于主机层面的泄露是 3 种泄露形式的源头,最为关键和重要,因此本书主要关注的是主机层面的隐私泄露。主机层面的隐私泄露主要是由各种含有隐私泄露行为的软件所致,这种软件我们称之为“隐私泄露软件”。这种软件分为两种主要类型:

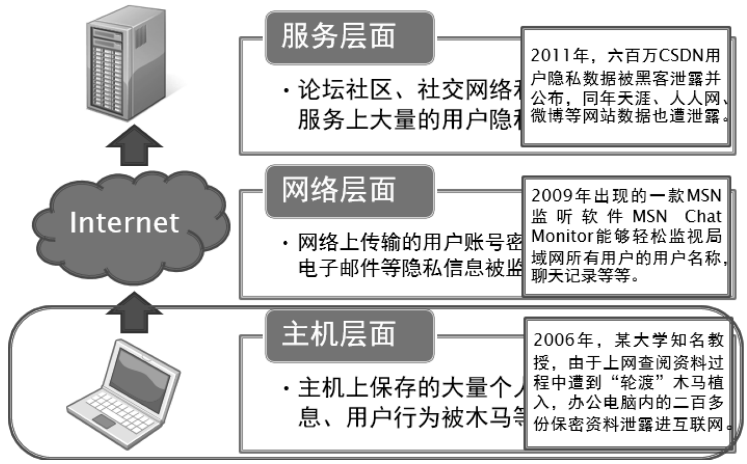

图 1.2.1　隐私泄露发生的 3 个层面

①由于隐私信息能够为攻击者带来可观的经济利益，对于隐私相关的当事人造成严重的影响，所以导致以泄露用户隐私信息为目的的恶意软件大量涌现；②在一部分常用的应用软件中，出于搜集用户个人爱好和消费习惯等商业目的，也暗藏了一些泄露用户隐私的功能。我们将这些软件统称为隐私泄露软件。

1.3　隐私数据泄露案例

1.3.1　“棱镜计划”隐私数据泄露事件

英国《卫报》和美国《华盛顿邮报》2013 年 6 月 6 日报道，美国国家安全局和联邦调查局于 2007 年启动了一个代号为“棱镜”的秘密监控项目，直接进入美国网际网络公司的中心服务器里挖掘数据、收集情报，包括微软、雅虎、谷歌、苹果等公司在内的 9 家国际网络巨头皆参与其中。2013 年 6 月 9 日这一天注定要被载入史册，一个名叫爱德华·斯诺登的美国人的现身让全世界的目光都聚焦到了香港，因为这个人，美国的最高机密监听项目——棱镜——被公之于众，令全世界哗然。

1.3.1.1　事件回顾

2013 年 6 月 5 日是“棱镜计划”事件的一个开端，英国《卫报》率先爆出 NSA（美国国家安全局）监听本国 Verizon 通信服务商用户通话记录的消息，指出他们获取到一条绝密命令的副本，内容为 NSA 命令 Verizon 每天向美国国家安全局提供公司系统中数百万用户全部通话的信息，无论是国内通话还是跨国通话。根据这份命令，美国政府将获得通话双方的电话号码、通话发生的时间、通话时长、位置数据等信息。不过

通话的内容并不在监控范围内。次日,《华盛顿邮报》给出了更猛的爆料,美国国家安全局和联邦调查局(FBI)正在通过一个代号为 PRISM(棱镜)的机密项目,直接利用美国九大顶级互联网公司的中央服务器,提取音频、视频、照片、电子邮件、文件和链接日志,以便帮助分析师追踪个人用户的动向和联系人。这也标志着“棱镜”项目首次公之于众。

2013 年 6 月 9 日,爆料人爱德华·斯诺登(Edward Snowden)在香港曝光,他作为中情局信息技术员派驻瑞士日内瓦并工作至 2007 年,在那里接触到一些机密文件。他说,自己在那段时间一度考虑公开那些秘密监视项目。不过,最后他决定放弃,原因是不想致任何人于危险之中,同时抱有对奥巴马当选总统后取消一些项目的期望。但是,奥巴马上台后并没有约束这些项目,这使他很失望。

斯诺登于 2009 年离开中情局,为戴尔计算机公司工作,随后作为博斯公司雇员在国安局工作 4 年。2013 年 5 月 20 日,斯诺登复制完最后一批绝密文件,告诉管理人员“需要离开几周治疗癫痫病”后便离开了夏威夷,之后藏匿在中国香港特别行政区。6 月 10 日,《外交政策》杂志曝光 NSA 下属黑客组织 TAO,该组织具有超凡的政治敏感性,过去 15 年中一直从事侵入中国境内计算机和通信系统的网络攻击行为,借此获取有关中国的有价值的情报。该组织创建于 1997 年,主要任务是针对美国以外的国家进行情报搜集和网络入侵。

“棱镜计划”是一项由美国国家安全局自 2007 年起开始实施的绝密电子监听计划。该计划的正式名为“US-984XN”。它是“星风计划”的 4 个子项目之一,泄露的文件描述 PRISM 项目能够对实时通信和既存数据进行深度监听。许可的监听对象包括任何在美国以外地区使用参与项目公司服务的客户,或是任何与国外人士通信的美国公民。

1.3.1.2 事件分析

“棱镜计划”直接利用了美国九大顶级互联网公司(包括微软、雅虎、谷歌、Facebook、PalTalk、AOL、Skype、YouTube、苹果公司)的中央服务器,电邮、即时消息、视频、照片、存储数据、语音聊天、文件传输、视频会议、登录时间和社交网络资料的细节都被政府监控。通过棱镜项目,国安局甚至可以实时监控一个人正在进行的网络搜索内容。通过分析可以看到下述事实。

• “棱镜计划”通过入侵大型路由器可以窃取主骨干网络上的信息

斯诺登在采访中透露,NSA 主要通过入侵大型路由器以窃取主骨干网络上的信息,无需对个人计算机进行逐一渗透。

如果要追溯历史的话,美国于 1994 年便通过了《执行通信援助法》,强迫所有的美国通信业制造商都必须遵守这个方案生产设备。像思科这样著名的美国通信业巨头,作为本土公司,要遵守这样的法律规定生产设备是理所当然的,况且思科正是发起并一直维持这个体系的公司之一。《卫报》和《华盛顿邮报》披露的 PRISM PPT 在

第3页中明确指出了美国作为世界通信网络主干的重要地位，可见，对主干网络以及国家边界路由器上的信息进行监听与捕获必然是棱镜项目获取机密信息的重要手段之一。

我国骨干网上的核心设备几乎百分之百都来自思科公司。思科到底有没有预留后门？目前并没有确凿的证据证明其有。但从另外一个角度来看，有没有后门并不是最关键的，真正可怕的是，一旦真正的网络战争爆发，如果对方有一种办法让我们的网络设备骨干网都瘫痪，比如一个bug便导致设备均不能工作，其所产生的杀伤力将无比强大，而这要比偷走信息容易得多。

- **“棱镜计划”可以从互联网公司的服务器获取数据**

因为《卫报》和《华盛顿邮报》披露了包括PRISM在内的两个任务的数据来源，对于“PRISM从美国服务提供商的服务器直接进行收集”的描述一时将这些互联网公司推向了风口浪尖。这暗示了有关部门能够通过某种方式登录谷歌、雅虎等公司内部的计算机，使用私有服务工具获取用户的数据。

《卫报》于2013年6月7日以“What Data Is Being Monitored and How Does It Work?”为题对PRISM使用IT公司的服务器作为数据源加以分析，结合《纽约时报》同日发布的“Tech Companies Concede to Surveillance Program”一文可以总结为以下几点：

首先，虽然入侵路由是获取信息的主要手段，但绝大部分信息流是加密的，要破解这些加密的传输信息，必须由相关公司提供密钥进行解密。

其次，2000万美元的年度预算能支持如此庞大的监听项目犹如天方夜谭，这让很多专家都感到非常困惑。互联网公司的日流量巨大，要存储相关服务器上所有的数据，如此低的预算根本不足以满足整个项目的开销。那么通过怎样的途径可以减少资源消耗呢？

综合各方媒体报道，NSA获取这九大互联网公司的数据可以概括为以下3个方面。

(1) 相关人员拥有管理员级别的查询接口

相关人员可以利用高权限的查询接口访问指定互联网服务器，按需索取，一旦发现感兴趣的信息，便将数据转储到本地，利用本地信息存储的方式减少开销。

(2) 特定服务器的安插

《纽约时报》提出了一种叫做“locked mailbox”的方式，即NSA在这些公司的服务器群中安装他们自己的服务器。一旦政府提出要求时，目标公司即将数据转移到lock-box中，使得NSA得以快速获取。

(3) Accumulo——NSA专门打造用于存储和分析庞大数据的开源数据库

Accumulo基于Apche Hadoop系统框架设计，类似于谷歌的BigTable存储系统，被认为是PRISM背后的关键技术。专家认为，PRISM基于现有软件和硬件技术，利用公众可用信息，完全可以实现追踪用户在线行为；Accumulo只需元数据，比如谁

打给谁，不需要知道此次会话具体内容就足够判断这些人的身份。对于任何通信方式，用语言处理算法打破内容句子和单词权重，通过程序可以实现对于意图信息的重现。

以上 3 种技术分析只是棱镜项目技术手段的冰山一角，该项目涉及国家机密，当然不会把大量的技术细节曝光于众，但我们可以确定的就是不仅限于这九大互联网公司，只要拥有数据的源头，一旦执行国家层面的情报收集命令，主动提供数据，一切的技术难题也都称不上难题了。比如，全球最大的软件公司——微软在公开发布补丁修复漏洞之前，就会向情报部门提供这些漏洞信息。这些信息可用于保护政府计算机，并入侵恐怖分子或敌对方的计算机。又如英特尔旗下的信息安全公司 McAfee 也被视为有价值的合作伙伴，经常与 NSA、FBI 和 CIA 合作，因为该公司能够了解恶意互联网流量的情况，包括外国势力的间谍活动。

1.3.2 搜狗浏览器隐私数据泄露事件

2013 年，搜狗浏览器被央视新闻曝光，指出其存在收集用户隐私数据，并致泄露的事件，引起了广大用户的关注。央视新闻中透露，该浏览器会记录用户的账户信息和登录密码，并通过网络上传到其他用户处。通过 QQ 登录该浏览器，可以查看到数千其他用户的个人账号，包括 QQ、邮箱、支付宝、银行等涉及用户财产的账户信息，可以直接进入其他人的支付宝进行转账购物，甚至直接支付交易。

1.3.2.1 事件回顾

2013 年 11 月，拥有几千万用户的搜狗浏览器，被曝光存在重大安全隐患，搜狗浏览器的自动填表功能会大量泄露用户私人信息。由于搜狗浏览器泄露的账号密码分类非常广泛，并且泄露时间持续至少 1 周以上。这是互联网浏览器历史上罕见的安全事故。中国最大的互联网安全公司 360 公司召开媒体沟通会，通报了此次由于搜狗泄密而导致重大安全事故的情况，公布了搜狗收集用户隐私数据并泄露的相关资料，并展示了完整的、经过法律公证的相关视频。

该视频显示，在一台只有基本应用程序的电脑中，下载安装搜狗浏览器，点击搜狗浏览器的账号登录系统，使用 QQ 账号和密码进行注册和登录，双击退出该系统。然后，在工具栏里单击“智能填表”，再选择管理表单数据，网页上就会弹出一个表单。继续点击，就会出现大量不同用户的个人账号密码等信息。视频显示，使用这些账号和密码能够进入到这些用户的淘宝、邮箱、QQ 等系统中。

此次能够获取到泄露数据的版本是搜狗浏览器 4.2 版本，但其他版本的搜狗浏览器登录账户和密码，都可能被泄露到使用搜狗浏览器 4.2 版本的用户电脑中。由于搜狗浏览器的自动填表功能是默认开启的，而且搜狗浏览器 4.2 版本已经作为正式版在推广，因此此次安全事件的影响面非常广。

360公司建议用户及企事业单位应尽快更换密码。对于曾经使用过搜狗浏览器自动填表功能的用户，目前必须要做的，就是第一时间修改所有登录或保存过的账号密码，包括但不限于电子邮箱、社交媒体、电商、电子支付平台、手机应用账户、政府信息管理系统、公用事业信息平台、电信服务、高校内部管理信息系统、企业内部管理系统等。

1.3.2.2　事件分析

该问题存在的技术原因在于该浏览器的智能填表功能存在着漏洞，会收集用户的登录账户及密码信息。而该浏览器会将用户保存的大量的账户信息、收藏夹内容等，自动同步到其他用户的电脑中。当其他电脑上的用户登录该浏览器时，就会自动地将这些同步信息下载下来，从而造成用户隐私信息的泄露。此外，一些国产的浏览器自身都存在严重的隐私问题。它们会收集用户的上网行为，如用户在什么时候访问了什么网站等，并且把用户的上网行为保存到指定的服务器上。一旦使用了有危险的浏览器，即使在其他方面的防范工作做得再好，也无济于事。因为浏览器是上网冲浪的关键，浏览器出现问题将导致隐私防御的全线崩溃。

总的来说，通过浏览器泄露用户隐私数据主要包括浏览历史和浏览器插件两个方面。用户的浏览历史主要包含网址的历史、下载的历史、页面缓存和各种Cookies等信息。虽然目前很多浏览器都支持隐私浏览模式，在“隐私浏览模式”下进行的上网行为，浏览器不会保存相应的“浏览历史”。当退出“隐私浏览模式”或者关闭浏览器之后，这些信息就不见了。但是，“隐私浏览模式”并不足够安全。如果浏览器安装了插件(比如Flash)，可能会导致“隐私浏览模式”部分失效。因为浏览器插件不受浏览器的控制。所以，即使在“隐私浏览模式”下，某些插件还是可能会留下上网痕迹。插件通常实现比较底层的功能，一般采用操作系统的本地代码编写，可以调用操作系统的API。形式上，插件以动态库的方式加载到浏览器的进程内。由于使用本地代码编写，插件通常依赖于特定的操作系统。

1.3.3　360软件隐私数据泄漏事件

1.3.3.1　事件回顾

2010年12月31日，普通用户在Google网站上搜索指定关键字，可以搜索到大量中国互联网用户使用互联网的隐私记录，甚至包括用户登录网站或邮箱的用户名、密码等。随后，金山公司召开发布会，称“360侵犯用户隐私”，并发布“一级安全预警”，称“上亿用户名和密码外泄”。金山公司在事件发生后，通过新闻发布会发布了多张隐私记录截图，宣称3亿网民面临隐私信息被窃取的风险，并发布安全预警。

经过360公司对网址云安全查询日志的统计，发现带有用户名和密码的数据的确

保存在了服务器上，通过访问 Google 也的确可以访问到这部分数据。虽然 360 公司已将这些数据删除，但是，由于该服务器可在互联网上直接访问，因而可能所有被上传的用户数据都已被各类黑客、电脑爱好者和潜在的破坏者下载，实际上已造成了不可估量的损失。使用 360 软件的用户应当及时更换密码。完全阻止隐私泄密是一件非常困难的事。一方面，使用防病毒软件，可以有效阻止隐私外泄；另一方面，不能轻易相信某个厂家的产品。

360 公司对此做出的回应包括：

(1) 导致此次事件的原因，是因为 360 存储网址云安全查询日志的一台内部服务器遭到了攻击，使得原本无法被搜索引擎抓取的日志数据被 Google 的爬虫抓取到了少量数据。经与 Google 搜索结果核对，一部分数据能在 Google 中搜索到，一部分在 Google 中搜索不到。360 公司正在调查，金山公司是通过何种途径得到放在 360 服务器上的恶意网页拦截日志的。

(2) 所谓“收集隐私”只是正常功能。上传可疑网址信息是安全软件的通用技术，很多安全软件都有类似功能。但是，金山自己的软件——“金山网盾”也会在用户访问可疑网址后上传网页浏览记录。安全软件在发现用户浏览器受到恶意代码攻击时，会将可疑恶意网址上传到服务器进行自动分析，然后把鉴定出来的挂马网址加入恶意网址库，这是安全行业通用的做法，除了金山和 360 外，诺顿、趋势等公司也都有类似的机制。

1.3.3.2 事件分析

定位到单个用户，该用户访问互联网的详细访问记录。360 软件会把用户访问的网址和 360 云安全中心的恶意网址库进行比对，以鉴别和拦截挂马、钓鱼、欺诈等恶意网页。针对单个用户的标识码 MID 是通过不可逆的随机算法生成的一个随机字符串，不可能反向推导出用户电脑的任何信息，因此并不涉及用户隐私信息。

该用户登录网站、邮箱、QQ 空间，少数网站在用户登录时，会将用户名和密码直接编写在 URL 网址中，传送给服务器进行身份验证。而 360 网盾与其他国内外安全软件一样，只查询 URL 网址，不会主动去识别其中的用户名和密码。

该用户进行的搜索行为的关键字信息，当用户使用多标签浏览器同时打开多个网页时，由于在同一个浏览器进程中打开了多个网页，360 网盾会将用户同时打开的多个网址 URL 一起上报至服务器，由服务器进一步甄别出其中的恶意网页。包括用户使用搜索引擎时，URL 中附带的搜索关键词。对于鉴别出的正常网页，其 URL 网址记录会自动地从日志文件中删除。

用户访问和使用企业内网的登录账号、密码、访问动作等，黑客/木马程序可能会构造 SQL 语句并加在 URL 中对网站数据库发起攻击，这种攻击请求会被 360 网盾截获，因此在日志数据中会看到极少量的 SQL 语句。