中文摘要

1890年美国的两位著名法学家萨缪尔 D·沃伦和路易斯 D·布兰代斯在《哈佛法律评论》第4期上发表了著名的《隐私权》一文，从此揭开了法学研究、立法和司法的一个新篇章。一百多年来，隐私权的法律保护成为众多学者研究的课题。隐私权直到近代才开始受到法治的认可和保护，是因为：只有在人类逐步摆脱贫困，不再因为物质条件的贫乏而影响其生存的时代，才会更多的将注意力转移到对其人格尊严包括对隐私权保护的关注方面，“人们在精神方面受到的痛苦和忧伤远远大于人们在极少情况下可能受到的身体损害的痛苦”。当今世界大多数国家在宪法和法律中都确认隐私权是一项独立的民事权利。《世界人权宣言》、《公民权利和政治权利国际公约》等主要国际人权文件也将隐私权作为一种人格权予以确认和保护。

但是现代科技尤其是电子信息技术的飞速发展和广泛运用，为大量的普遍的侵犯隐私权的情形创造了物质条件，特别是个人数据信息隐私权更容易受到侵犯，使得对公民和机构团体隐私权的保护变得更为迫切。因此，深入探讨隐私权法律制度，特别是研究网络时代如何完善我国公民隐私权法律保护问题，是非常必要的。本文分析了网络中个人数据隐私权受到侵犯的各种现象，借鉴国外的相关保护经验，对我国网络个人数据隐私权的法律保护提出了应对措施。全文分前言、正文和结束语三部分，正文共分四章：

本文第一章描述分析了网络发展对个人数据隐私权的挑战，21世纪的今天，网络时代的飞速发展在给人类带来无数便捷和利益的同时，也给隐私权保护带来巨大的挑战。网络时代，凭借高科技手段，人们对他人隐私的获取和侵犯变得轻而易举，网络空间的隐私权比物理空间的隐私权更难设防、更难控制，高速运转的“无国界”的互联网正面临着日益严重的信息泄露和隐私权侵犯问题，个人数据隐私遭到侵入、截取、篡改、插入、删除、披露、非法利用等多种威胁，因此必须建立完善的信息安全体系，从法律上保障公民的隐私权，抵制各种不法侵害。这部分重点阐释了个人数据的概念和法律特征，结合

其他国家的相关概念，将个人数据定义为：“个人数据是指自然人（包括由自然人组成的家庭的整体）已经被识别或可以用来识别的个人化信息资料。”它的内容包括个人自然状况、社会与政治背景、生活经历及习惯、家庭基本情况等。个人数据的特征是：个人数据为生成该数据的自然人主体所拥有；数据主体必须是可以识别的；个人数据的范围非常广泛；数据用户使用个人数据必须限定在批准范围或事先声明的使用范围内；获取个人数据必须事先经过批准或得到同意且使用合法手段。并进一步从法律地位、客体、权能三个方面将个人数据隐私权与传统隐私权进行了对比。

本文第二章从历史和发展的角度阐述了世界发达国家，主要是美国，欧盟等经济发达国家在网络时代的隐私权保护立法。欧盟的《数据保护指令》在电子商务的隐私权保护立法方面最具有代表性，指令的两个基本目的，一是保障自然人的基本权利和自由，尤其是隐私权，二是确保信息在成员国内自由的流动。美国对网络个人数据隐私权采取的主要是行业自律政策，制定和实施隐私条款则是业界进行行业自律最常见也最基本的自我约束方式。具体又包括业界自律和第三方认证两种形式。自律手段和法律手段分别是保护网络隐私权的两种最主要的手段，但是它们也都有各自的优点和缺点。对于法律手段来说，尽管法律具有稳定性、可预见性等性质，但它同样存在僵化性，而在网络和电子商务的飞速发展的今天，要制定出完善的法律制度，无疑对立法者的要求很高。对欧盟的数据保护指令来说，虽然具有明确性，但是它自身还存有一些问题，比如它的适用范围在实践上的不确定性，指令的保守倾向也比较明显。对于美国的自律手段来说，也存在监管困难，缺乏强制力和法律救济体系等问题。因此这两种个人数据隐私权保护手段都各有利弊。

本文第三章是论文的重点，论述了侵害网络个人数据隐私权的社会学分析和侵害构成要件。对于侵犯网络个人数据隐私权的行为，其根本的动因是为了获得经济上的收益，现代社会中数据信息已经成为一种商品，各种经济活动对用户个人信息的要求也越来越详尽，必须在满足大量的个人信息需求与保护个人网络隐私权之间寻求平衡，这

是我们需要关注的焦点。侵害网络个人数据隐私权的主体主要是商业公司和黑客，侵害的行为包括两大类：一是非法获取信息；二是不恰当地共享或披露用户信息。这两类侵害行为主要是技术上的手段，比如使用木马程序，在免费软件内安插广告等。在论述了侵害行为之后，进一步提出侵害网络个人数据隐私权是一种可赔偿性损害。个人数据是网络隐私权最重要的客体 and 表现形式之一，在网上对个人数据的非法采集、利用和不恰当地披露就构成对网络隐私权的侵害。侵害个人数据隐私权的行为和侵害网上其他人格权的行为既有联系也有区别，而且可能构成竞合，比如侵害网上肖像权的同时也可能构成侵害个人数据隐私权。侵害个人数据隐私权，必须具备主观过错要件，在故意和重大过失的情况下，造成对他人隐私的侵害，就应当予以赔偿。侵害人一旦构成侵权行为，就必须承担相应的民事责任，包括停止侵害，赔礼道歉，赔偿损失等等。赔偿损失是侵害个人数据隐私权应当承担的一种最主要的民事责任，就赔偿的范围而言，应该包括两个方面，一是对受害人受到的精神损害应当进行赔偿，二是对受害人因隐私受到侵害而产生的其他损害的赔偿。但是在受害人同意，或为了社会公共利益而需要公开他人的个人私事以及发生意外事故的情况下，公开他人的隐私构成阻却违法，不承担民事责任。

本文第四章综合考察了我国隐私权法律保护的现状，我国受历史传统等因素的影响，个人隐私权长期以来没有得到应有的重视，我国大陆地区也没有构筑出完整的隐私权保护法律体系，隐私权并未成为民法上一项独立的权利。尽管我国宪法、民法等法律以及最高人民法院的相关司法解释或多或少涉及了公民隐私权及其保护，但从总体上看，隐私权还没有成为我国法律体系中一项独立的人格权，更不用说对网络个人数据隐私权的保护。因此建议应从我国国情出发，在制定网络空间隐私权保护制度的时候，应以法律法规、行为规范和技术应用为基础，采取立法为主，自律为辅的保护模式。首先必须完善民事立法，在制定民法典的时候，应将隐私权明确纳入人身权的保护范围，确认隐私权为独立的诉因，规定侵害隐私权应承担的民事责任。民法典多为原则性规定，需要各种专门法加以补充。因此需要制定专门的

数据保护法，其内容应该包括数据收集主体，收集者的义务，数据主体的权利，公用记录的特殊保护，侵权救济等方面。综上所述，在民法领域建构较完善的隐私权保护制度，再以此制度统领数据保护规范中对网络个人数据隐私权的具体规定，这样才能切实维护公民的网络空间隐私权。

本文的创新之处在于对网络个人数据的概念范围进行了详细分析，在与传统隐私权的比较下，结合传统侵权行为法的构成要件，提出了侵害网络个人数据隐私权的侵权构成要件，包括主体、行为，主观过错，损害事实等。并阐述了侵害网络个人数据隐私权是一种可赔偿性损害。

关键词：个人数据 隐私权 网络隐私权 个人数据隐私 可赔偿性损害

Abstract

In 1890, two famous justice scholars of the United States of America, published their famous article — 《The Right to Privacy》 in the fourth issue of 《the Harvard Law Review》, which announced the new age of the research method. More than 100 years in the past, the law protection of the right to privacy becomes the topic that numerous scholars began to study. Until in modern age, The Right of the privacy was just confirmed by the rule of law and its protection. Nowadays most countries of the world all confirmed that the right of privacy in constitution and laws is an independent civil right. The main international human rights document, such as 《The Declaration of Human Rights》 and 《The International Convention of the Citizen Right and Political Right》 all confirmed that the right of privacy is one kind of personality right and should protect it.

But the development of internet and E-commerce has taken huge menace to people's the right to privacy. Therefore, the problems of the right to privacy attract more and more attention of the user of internet. On the base of analyzing the meaning of the right to privacy of personal data, the article points out the forms of infringing the right to privacy of personal data in internet and E-commerce at present. On the same time, using the measures that foreign countries have taken for reference, the article forward how to protect the right to privacy of personal data in internet and E-commerce according to the fact of our country.

This article analyzed the network in various phenomenon that the right to privacy of personal data be subjected to infringe upon, drawing lessons from the related protection experience of foreign countries, and put forward to reply the measures to personal law of data right of privacy of network of our country. The full text contains three parts: the foreword,

text and postscript, the text is divided into four chapters:

Chapter one analyzed the network development to personal challenge of the right to privacy of personal data, in 21st century, the rapid development of the internet not only bringing numerous conveniences and benefits for mankind, but also bring huge challenges for the right of privacy protection. Network ages, with the high-tech means, obtain to the others' privacy becomes easy to accomplish with invasion, the right of privacy of the cyberspace is much more difficult than the right of privacy of the physics space to establish to defend, more difficult to control. The Internet of the high-speed operation faces the increasingly serious information to reveal face to face to infringe upon the problem with right of privacy, personal data privacy encounters the incursion, intercept, distort, insert, delete, publishes, illegal make use of and other various threats of etc., so we must build up the safe system of perfect information, from the right of privacy that the law guarantees the citizen, boycott various illegality to violate. This part of points explained personal concept of data and the law characteristics, the related concept that combines other nations was also further to carry on the right to privacy of personal data and traditional right of privacies from the point of law.

Chapter two elaborated flourishing nations in the world from the angle of the history and development, mainly the United States, the economic flourishing nation of etc. EU is in the right of privacy protection lawmaking of network ages. 《The Data Protection Instruction》 of EU is the representative in the the right to privacy of the protection in the lawmaking in the electronic commerce. There are two basic purposes of the instruction, basic one is the right and the freedoms that guarantee natural person, basic two is to insure the information at the free fluxion of member. The United States is mainly adopt the profession self-discipline policy to protect personal data right of

privacy .The self-discipline method and the law method are the two main methods that protect the network right of privacy respectively, they each have advantages and disadvantages.

Chapter three is a textual point of this article, discussing the violation of personal composing important item of data right of privacy of network, violating the corpus is mainly the business company and hackers, express the behavior is divided into two kinds, first the right and wrong method obtains personal data information, second is illegal share or publish personal information of customer fittingly. And further analyzed personal data right of privacy of network of invasion is a kind of compensation damage, only being to violate the person intentionally or grievous fault then can affirm in order to constitute the infringement, and victimize the square to only prove that the property loses up and then can acquire the indemnity.

Chapter four synthesized to investigate the present condition of our country's right of privacy law, though the related judicatory of the law and Supreme People's Court of our country constitution, civil law was hermeneutic many or little to involve the citizen right of privacy and its protect, from totality, the right of privacy have not yet become an independent personality rightt in our law system, saying nothing of the protection to personal data right of privacy of network. Therefore we should be perfect our cyberspace personal data right of privacy lawmaking, specify the homologous laws and the profession self-discipline measures as soon as possible, then can promote the network civilization developped quickly and healthily.

Key words: Personal data

The right to privacy,

The right ro privacy on the internet

The right to privacy of personal data

Compensation damages

西南财经大学

学位论文原创性及知识产权声明

本人郑重声明：所呈交的学位论文，是本人在导师的指导下，独立进行研究工作所取得的成果。除文中已经注明引用的内容外，本论文不含任何其他个人或集体已经发表或撰写过的作品成果。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。因本学位论文引起的法律结果完全由本人承担。

本学位论文成果归西南财经大学所有。

特此声明

学位论文作者签名：向欣

2005年4月22日

前言

电子商务经过多年的发展，已取得了长足的进步，网上贸易额逐年增加，长势强劲，这在一定程度上得益于其所依托的媒体——计算机网络的高度开放性，使传统贸易中最为棘手的跨地域问题大大缓解。信息是一个国家最重要的经济资源。在市场和竞争日益全球化的今天，拥有制作、操作、管理和使用信息的技术对任何一个国家都是非常重要的。现在，大部分信息都是电子的或是数字的。由于信息采用了这种数字或电子的形式，使得我们处于一个信息爆炸的时代。首先，由于新技术的出现，信息的采集、管理、传输和储藏都比以往更加容易；其次，信息的采集、管理、传输和贮藏的成本也比以往降低了；再次，数字化的信息本身有很多优势，比如内容详尽，可以重复使用和使用方便等；最后，数字化信息正在许多领域改变交易的方式，如银行的结算业务已经实现无纸化，只需进行数字交换即可。由于以上优点，不仅有越来越多的数字化信息产生出来，而且人们对数字化信息的依赖性也越来越强。

信息技术的飞速发展在给人们的生活带来极大便利的同时，也产生了诸多的法律问题：1、知识产权。如何确定数字化信息的所有权以及如何适用现有的知识产权法尚待研究。比如，谁拥有数据库的所有权就是一个比较棘手的问题；2、言论和出版自由权。法律保护言论和出版自由权，同时也加以合理的限制。网络的出现使人类社会又增加了一种新的传媒，如何对充斥在网络中的各种数字化的言论加以保护和限制成为原有法律制度面临的新问题。3、国际立法管制。数字化的信息的一个重要特性就是无国界性。由于网络的存在，信息可以在世界范围内广泛的流动。人们很难查出信息源自何处并对其传播加以阻拦，电脑病毒多次在全球爆发就是一个很好的例证。4、隐私权。在新技术信息条件下，隐私权是指对数据信息的传播和使用的控制权，包括特意披露的信息和使用信息技术时不经意泄露出来的信息。这就对数据贮藏、处理和传输系统提出了很高的要求，以防未被授权使用者的入侵。对数据信息

加密和解密是解决这一问题的技术手段，但技术手段并非万能的，黑客在网络中的恣意妄为就证实了这一点。网络时代凭借高科技手段人们对他人隐私的获取和侵犯变得轻而易举。网络空间的隐私权比物理空间的隐私权更难设防，更难控制。高速运转的无国界的互联网络正面临着日益严重的信息泄漏和隐私权侵犯问题。个人隐私遭到侵入、截取、篡改、插入、删除、披露、非法利用等多种威胁。因此必须建立完善的信息安全体系从法律上保障公民的隐私权，抵制各种不法侵害。网络时代也改写着有关隐私权的法律概念，个人数据隐私权的概念应运而生。

尽管我国宪法、民法、刑法、刑事诉讼法、民事诉讼法、其它行政法规法规以及最高人民法院的相关司法解释或多或少涉及了公民隐私权及其保护，但从总体上看隐私权还没有成为我国法律体系中一项独立的人格权。公民隐私权保护以及对隐私权侵权诉讼也没有形成专门的法律制度。司法实践中，公民隐私权受到侵害不能以他人侵犯其隐私权为诉因直接提起诉讼，而只能以相应的人格权（通常是名誉权）等民事权利受到侵害为诉因请求法律救济与保护。这对公民隐私权的保护无疑是不充分不全面的，且保护力度也大打折扣。因此有必要对网络上个人数据隐私权问题做深入的探讨和研究分析，在参考借鉴国外先进立法经验的基础上，总结和探索适合我国国情的个人数据隐私权保护制度，从而为我国研究个人数据隐私权问题，适应我国社会经济的发展 and 公民对人身权法律保护的要求，适应世界各国对隐私权的法律保护体系日趋统一的大潮流，建立符合我国国情的隐私权法律保护制度，完善我国的人格权制度尽绵薄之力。

科学的理论建立在科学的研究方法之上。我将运用实证与规范相结合，以民法基本理论为指导，以相关计算机数据科学、社会学知识为依托，以比较法上发达国家的先进立法经验和理论为背景，结合我国实际情况，对网络中个人数据的隐私权保护进行深入研究，重点在于结合传统民法中侵权行为理论，对网络中个人数据隐私权侵权的构成要件进行分析，并对侵犯个人数据隐私权之原因和后果进行社会学的考察，在整个论文中将贯穿网络中个人数据隐私权与传统民法隐私权各方面的比较，进一步深入探讨个人数据隐私权的性质和特点。

第一章 网络时代的挑战与个人数据隐私权概述

（一）网络发展对个人数据隐私权的挑战

二十世纪最具影响力的创新莫过于人类拥有了处理大量数字化信息的技术。计算机和网络在全世界范围内对商业、教育、休闲乃至社会生活的各个方面的发展都起到了迅猛的推动作用。“信息是一个国家最重要的经济资源。¹在市场和竞争日益全球化的今天，拥有制作、操纵、管理和使用信息的技术对任何一个国家都是非常重要的。现在，大部分信息都是电子的或是数字的。文字利用字处理软件来编辑，储存在电脑的内存中，通过电话线、卫星传输，用打印机、传真机打印出来。图象和声音由摄影机、扫描仪、DV机、话筒等采集，储存在磁带或光盘中，通过光揽传输，用电视、电脑或收音机播放出来。事实上，涉及远距离和面向大众的信息传输都离不开数字化、电子信息技术，而且其发展速度和规模是惊人的。

在现代科技手段，尤其是信息技术的帮助下，个人数据隐私也同其他信息一样能够以“0”和“1”的数字形式被无损坏的复制和传播。在网络上，这种复制和传播的能力甚至几乎是无限的。然而，隐私作为一种信息，它的特殊之处又在于它本身应当被任意复制和传播。网络的出现和迅速的发展，无疑给个人数据隐私权的保护带来了前所未有的巨大威胁。

具体说来，网络对个人数据隐私权的冲击主要表现在：较之以往的技术手段，它使得个人信息能够被更容易地获取和更加广泛地传播，而侵犯隐私权的行为却更难以察觉，侵犯的后果也更加严重。网络的突出特点之一在于它的开放性，借助强大的搜索引擎，几乎任何希望得到的信息，当然也包括个人信息，都可以轻松获取；同时也正是由于这一特点，只要个人隐私被载于网上，在这个访问者无数又没

¹ Information Infrastructure Task Force, National Information Infrastructure Agenda for Action 5(Washington, 1993)

有物理疆域概念的虚拟社会，它的传播就可能比火箭速度更快，“航程”更远。可是，与获得和传播个人隐私的“易”相比，想在网络的海量信息中主动觉察到个人数据隐私权受侵犯的蛛丝马迹，可谓“难”而又“难”。而且即使这种行为能够被敏锐地发觉，其始作俑者也难以追查，因为只要拥有了电脑、电话线和调制调解器，并且具备了必需的技术知识，任何人在任何地方都可以在网上完成结果完全一样的操作。当然，最引人关注也最令人头痛的还是隐私权受到侵犯后可能产生的后果。以往的技术手段由于搜集和传播信息的能力有限，即使对隐私权造成侵害，其影响也通常局限于一定的范围内。例如，当某人的银行帐号信息被窃时，窃取者所能知道的不过是被窃者的帐上有多少钱，如果手段高明的话，最多玩点伎俩，把钱全部归入自己囊中。至于银行帐号与个人社会经历或健康状况之间会有什么联系，恐怕打破了脑袋也想不出来。可是在网络上，各种有关个人情况的数据库彼此相互联系，任何细微的线索都可能经由网络引出一连串详尽的个人描述，这时的上网者所面对的因个人数据隐私泄露而带来的损失便不再是局部的，它甚至可能让受害者付出生命的代价。

Amy Boyer 是居住在美国 New Hampshire 州的一位年轻女性，她怎么也没有想到，一次偶然的网上邂逅竟最终夺去了她的生命。1999 年秋天，Boyer 在网上结识了一个名叫 Liam Youens 的男子，这名男子结识了 Boyer 后便一直尾随她，他先用 45 美元从 Docusearch.com 网站购得了 Boyer 的社会保险号码，而后又通过这些信息在网上轻松查到了 Boyer 的工作地点，然后他找到那里开枪打死了 Boyer，然后饮弹自尽。²Youens 行凶的原因我们不得而知，但是有一点却非常明白，那就是：假如没有网络，Boyer 便不可能认识 Youens；即便二人有机会认识，如果没有网络，Youens 也不可能轻易地得到 Boyer 的社会保险号码和其他个人信息，并将其命送黄泉。尽管网络本身并无过错，可它在这一系列侵犯个人隐私权的行为中的确扮演了极不光彩的“帮凶”角色。

² 屈志辉《网络侵权行为法》，电子商务出版社 1998 年版，第 77 页

（二）个人数据的概念及法律特征

在网络时代的今天，网络对公民隐私权的保护提出了巨大挑战。如何有效保护公民的隐私权特别是个人数据隐私权，成为社会各界共同关心的问题。这更是诸多法律界人士重点研究的课题。

目前，世界不少国家和地区将个人数据明确为隐私权对象，并对个人数据作出了法律界定。瑞典在 1973 年制定的数据法和美国在 1974 年颁布的《个人隐私法》中对个人数据都有明确的表述。英国在 1984 年制定的《数据保护法》对个人隐私权的规定相对全面、完整，较有代表性。《数据保护法》规定：“个人数据是由有关一个活着的人的信息组成的数据。对于这个人，可以通过该信息，或者通过数据用户拥有的该信息的其他信息识别出来。该信息包括对有关该个人的评价，但不包括对个人数据用户表示的意图。”1995 年通过的《欧洲联盟数据保护规章》对个人数据下的定义是：“有关一个被识别或可识别的自然人（数据主体）的任何信息；可以识别的自然人是指一个可以被证明，即可以直接或间接地，特别是通过对其身体的、生理的、经济的、文化的或生活身份的一项或多项的识别。”借鉴上述国家以及欧盟的法律规定，个人数据的概念可以如此表述：“个人数据是指自然人（包括由自然人组成的家庭的整体）已经被识别或可以用来被识别的个人化信息资料。”个人数据的内容包括个人自然状况、社会与政治背景、生活经历及习惯、家庭基本情况等。其主要法律特征如下：

1. 个人数据为生成该数据的自然人主体所拥有。即这些数据是有关“个人”的。这个个人既包括自然人，也包括由自然人组成的家庭整体。有关公司、企业等法人或者非法人组织的信息不是个人数据；但是，英国 1984 年《数据保护法》规定，在商业中自负盈亏的人们（包括一些独家经营的商人们），都是一些个人，因此能成为数据主体。个人数据既包括活着的个人的信息，也包括已经死亡的个人的信息。但英国 1984 年《数据保护法》规定“个人数据是由活着的个人的信息构成的”。需要特别指出的是，个人数据只能为生成该数据的主体

所拥有。数据主体是指个人信息被收集为数据的自然人，即数据主体是该数据所针对的对象，而不是该数据的用户。数据用户是指合法收集，有限度地控制、使用有关数据的个人或组织。明确个人数据主体是生成该数据的自然人，这是保护个人数据的必要前提。也许单一或少量的个人信息被收集、输入数据库对用户而言并没有太大的价值，但是一旦数据库所容纳的数据超过一定量之后，数据的价值就越来越大。数据用户不经数据主体同意，在整体上使用个人数据（如对学生群体的考试成绩进行统计分析）是允许的，法律所禁止的是未经主体许可披露个人数据，如将学生的考试成绩张榜公布，或将特定的个人数据挪作他用。这是因为，数据用户对个人数据的控制权、使用权仅限于合同约定的范围；个人数据为数据用户控制、使用时，并不意味着主体放弃对该数据的所有权。

2. 数据主体(data subject)必须是可以识别的。按照英国 1984 年的《数据保护法》的规定，“数据主体”指的是其个人信息被作为数据加以收集的自然人。也就是说数据主体并不是作为数据库拥有法律主体，而是有关数据所针对的对象。只有通过数据中所反映的各种信息，以及加上人们的判断而可以确定某些数据是有关某个个人的，也就是说，通过数据中的信息是可以识别出数据主体的，这样的数据才是个人数据。个人数据不能是无名数据，例如，为统计的目的从有关的不确定身份的个人处获得几组数据，这些数据虽然出现每个人的名字，但这仍是个人数据，因为这些数据可以从其他地方核查而发现他们的身份：所以收集数据的公司不能通过获取数据主体的信息，却不出现他们的名字来避免法律的适用。相反，公司持有一些数据，例如是关于工会成员中的黑人、罗马天主教徒或者性变态者的比例的，那么就不认为是持有个人数据。因为这些数据不会导致认出该人的身份，然而，如果在雇员名单中只有一个黑人，那么这一信息会使此人被“认出来”，因此该数据就成为个人数据。

对数据主体的识别可以是直接识别，也可以是间接识别。所谓直接识别就是直接通过数据中所反映出的数据主体的直观特征加以识别，如数据主体的名字、照片、编号等往往无需加以核查或复杂的判

断；所谓间接识别就是必须得通过分析、核查、比较有关数据主体的身体的、生理的、智力的、经济的、文化的或社会身份的多项的信息后能判断出数据主体的识别。例加上例中的识别就是间接识别。还有如数据中包含一个密码或代号，通过它再参考你占有的其他资料，才能把主体识别出来。

3. 个人数据的范围非常广泛，足以对主体构成识别的数据均为个人数据。凡是个人身世、血缘、健康、财产、婚姻、经历、通讯、日记、住所地址和私人文件，包括存储在计算机内的个人信息等均属个人数据。总之一切与个人有关的信息，只要其能够构成对个人进行识别的信息都是个人数据。随着现代科学技术的发展，个人及其家族的基因图谱也应当纳入隐私权的保护范畴。具体地说个人数据又可以按照不同标准分为单一数据与组合数据、显性数据与潜态数据、静态数据与动态数据，等等。在多数情况下单一数据难以对个人加以识别，但是，若干个单一数据的组合就足以对个人进行识别；显性数据容易被发现（如身体暴露部分的疤痕斑痣等），潜态数据一般需要特殊方法提取（如每个人都有不同的基因图谱）；静态数据大多表征个人以往的情况，动态数据主要反映个人当前的状态（如现实的收入与支出）。故此，组合数据、潜态数据、动态数据的泄漏与传播对个人隐私的危害甚大。个人数据有的呈现为法定记载（如刑事犯罪记录），数据用户为其保密是无庸置疑的。但是，这决不意味着只要个人自愿提供了个人数据，用户就可以随心所欲地使用或将个人数据转让他人。用户一旦超越事先约定的范围使用个人数据就构成侵权，尤其是由若干单一数据组合成的数据串（组合数据），对个人具有极强的识别功能，更不允许数据用户任意泄露或者超越权限使用。

4. 个人数据不包括任何用户意图的表示。这仅仅是用户的意图不包括在其中，而不是第三者对数据主体的意见。尽管意图本身不是个人数据，但任何其他已经做为那种意图基础的个人数据，却没有被排除在个人数据之外（例如，履行信用的程度）。在遵照数据主体提出获取的要求时，这些数据应当予以透露。

5. 数据用户使用个人数据必须限定在批准范围或事先声明的使

用范围内。数据库的种类纷繁多样，各具用途。个人数据的本质并不是为数据库“充数”，而是对数据主体的识别。未经主体许可，任何人以明示或隐喻的方式披露个人数据都是非法的。这是因为即使采取不指名的方式，个人数据所反映的信息在特定的范围或条件下，加上人们的推测就可以识别数据主体。

目前，商业机构掌握个人数据的数量呈现膨胀之势。根据信息的效益递增规律，当数据用户掌握信息的质和量达到一定程度后，该信息就会给用户带来不断增多的效益，效益的递增率随信息的应用范围扩大而上升。我国某电子集团公司要求消费者在购买商品后，“详细填写用户档案卡，并在购机后一个月內寄来我部……我们将把您的有关资料存储于电脑中”。这显然是获取个人数据的行为，如果该公司将获取的个人数据用于产品售后服务当然无可厚非，若挪作他用就会造成对消费者个人数据隐私权的侵犯。例如，当消费者填写了一份某种商品的保修单之后，其它无数种商品的宣传广告、订购单就会纷至沓来。显然，消费者的个人数据、姓名、通讯地址等，此时已经被泄漏或被移作他用。从法律意义上说，当消费者为特定用途向特定对象提供个人数据时，只要数据用户接受这一数据，就是承诺了数据提供者的约定。数据用户只有在约定范围内使用该数据的权利，否则就是对个人隐私权的侵犯。

6. 获取个人数据必须事先经过批准或得到同意且使用合法手段。数据用户可以是个人，也可以是组织。但是数据用户未经事先登记批准擅自收集个人数据是不能被允许的，即使经过合法批准的个人数据调查，也应当事先公开调查目的。禁止以强迫、诱骗、收买、转让等手段取得个人数据。在互联网中，网络用户也许会收到来历不明的电子邮件，而且有免费的礼物引诱用户打开扩展名为“.zip”、“.exe”、“.scr”的文件。然而，一旦文件被打开，网络用户的个人帐号、密码就会被自动传送到这个被称为“特洛伊木马”的电子邮件发送者那里。这显然是以欺骗的办法窃取个人数据，严重侵犯了数据主体的隐私权。英国1984年《数据保护法》第五条规定，只有经过登记被批准为数据使用人（或数据使用人兼计算机中心）之后，该人才有

权持有个人数据。我国目前尚无收集个人数据的登记批准制度，这个立法空缺应当尽早弥补。

（三）隐私权概说

隐私有不同的称谓，法国法称之为个人生活，日本法称之为私生活，台湾有的学者称之为秘密，有的学者称之为隐私。构成隐私必须具备两个条件。首先是“私”，即指纯粹是个人的，与公共利益、群体利益无关的事情；其次是“隐”，即某件事情、某个信息不为人所知，或某种活动及领域不被他人干涉或侵入。

在人格权类型化的进程中，隐私权出现得较晚。学术界通常认为，1890年美国私法学者布兰戴斯和次伦在《哈佛法学评论》上发表的《论隐私权》一文，是首次提出隐私权的概念和理论。两位学者指出，紧张而又复杂的社会生活曾推动过人类文明，但经过文明熏陶的人们，对公开化变得更加敏感，因而隐私权对人们来说变得更加重要。在此后，隐私权理论在其他国家中也得到了发展。此项权利不仅被许多国家纳入法律保护的范围，而且也引起了国际社会的广泛关注，对隐私权的保护呈现出国际统一化的趋势。

尽管隐私权概念问世已有一百余年，但迄今为止没有一个公众所普遍认同的隐私权定义。国内目前有代表性的观点有：一种观点认为隐私权是自然人享有的对其个人的，与公共利益、群体利益无关的个人信息、私人活动和私有领域进行支配的具体人格权。³另一种观点认为隐私权是自然人就自己个人私事、个人信息等个人生活领域内的事情不为他人知悉，禁止他人干涉的权利。⁴再有一种观点认为隐私权是指私人生活安宁不受他人非法干扰，私人信息保密不受他人非法搜集、刺探和公开的权利。⁵可以认为，隐私权是指自然人就其个人私事、个人信息等个人生活领域内的事情不为他人知悉或不愿为他人知晓，禁止他人干涉的一种独立的人格权。

³杨立新《侵权行为法》下册，吉林人民出版社1998年版，第768页；

⁴王利明等《人格权法》法律出版社1997年版，第147页；

⁵张新宝《中国侵权行为法》（第二版），中国社会科学出版社，1998年版，第358页。

(四) 网络个人数据隐私权与传统隐私权比较

1、关于二者法律地位之比较。传统民法中的隐私权在人身权系列中处于较不显著的地位。在我国,将隐私权作为一种独立的人格权,是经过了学界长期的讨论之后,现在才确定下来的,但至今在我国的法律中还没有做出明确规定,实务中仍采取不同的做法。而网络与电子商务中的隐私权在将来的网络法与电子商务法律体系中则是一种基础性的权利。这主要是由网络与电子商务本身的特点决定的。

相对于我们现实存在的物理世界而言,网络最大的特点在于它是一个“虚拟空间”。物理世界里我们可以有房子、有汽车,我们看得到某某人长什么样子。在“虚拟空间”通常不是这样,有更多的虚拟性。首先它的主体,可能和我们在网上对话的不是一个人,而是一台终端机器,就象我们在银行的 ATM 机上去取钱的时候和我们对话的是机器,这是种没有人的存在。第二种情况是这个人是在存在的,但是他可以用一种虚假的身份和我们对话,最容易出现的是在聊天室里面和 BBS 上面,我们也可以隐瞒自己的身份和状况。这样对社会人际关系是有很大的影响的。我们自己总以为隐蔽自己的面孔别人就看不清我们真实的面孔,这时候我们有可能会在网上说真话。比如同事之间彼此太熟悉了有些话不愿意说,陌生人之间反而容易说真话,有时候在网上聊天和陌生人聊得很来劲,但是面对别人我们更容易说假话,因为别人没有办法去查证我们到底说的是真话还是假话。网络的这种虚拟性不仅仅包括在主体的虚拟性,还包括场景的虚拟性,关系的虚拟性。有时候一个网站给我们设置了很多场景,但是是虚幻的,在里面很多关系是虚拟的,比如有网上“情人”等。这些虚拟的场景和人际关系又不能完全与现实社会隔离开来,它们是相互影响的,会影响我们的情绪,我们的思想感情,甚至会影响到我们的家庭关系。⁶

因此网络虚拟社会有效运行的基础是不同于现实社会的。在现

⁶张新宝:《互联网发展对隐私权保护的挑战与对策》,
<http://www.privatelaw.com.cn/new2004/shtml/20040517-001910.htm>

实社会中,人首先是物质性的存在,有了人才有了人类社会各方面的活动,传统民法对于自然人的保护正是基于此而设定。这从人身权利种类的排列顺序(生命权—健康权—姓名权—肖像权—名誉权—隐私权)中可以清晰看出,对于有形人格权益的保护居于重心,而无形人格利益的保护则次之。这完全由现实社会的法律要求所决定。但在网络虚拟社会中,人的物质性被隐去,人与人之间,从事网上的一切活动,并不发生任何现实的身体接触,一般不会发生生命危险或身体健康遭受损害。虚拟社会的有效运行,全依赖于可识别的个人数据。而要使虚拟社会有效运行,则必须首先要保护好个人数据。实际上,也就是要保护好个人的隐私权。所以,在网络法体系中,个人的隐私权必然是首先应当保护的一种基础性的权利。

电子商务是网络应用发展的重点内容。电子商务获得良性发展的关键是保障交易者的信息安全,否则便会抑制电子商务的发展。2001年,位于纽约的 Jupiter 通讯公司发布的一份报告表明,由于用户担心网上隐私权受到侵害,将导致潜在的电子商务交易率收入降低 180 亿美元,广告收入下跌 27 亿美元,人们最为担心的是信用卡信息泄露和个人信息被售给第三方。所以,要保障电子商务的发展,就必须首先要保障个人信息的安全,也就是保障个人的隐私权不受侵犯。这样,隐私权必然成为电子商务法律体系中最基本的权利。

2、关于二者客体的比较。网络与电子商务中隐私权的客体,是网络中已被识别或可被识别的一个自然人的所有信息。它与传统隐私权的客体相比有以下不同:

(1) 两客体所处环境不同。传统隐私权的客体是处在现实世界中,而网络与电子商务中个人数据隐私权的客体则在虚拟世界中。

(2) 两客体的内容范围不同。传统的个人隐私包括:姓名、出生年月日、身份证统一编号、婚姻、家庭、教育、病历、职业、财务情况、特征、指纹等数据。随着网络的盛行,许多新兴的个人数据成为了隐私权所保护的内容,例如电子邮件地址(email address)、网域名称(domain name)、用户名及通行码(username 及 Password)、网际网络通讯协议地址 (IP address)等等。而且,随着科技发展日新月异,传

统社会中许多不认为是隐私权的内容在网络世界中都成为名副其实的隐私。在网络世界中只要能被识别的自然人的信息,都能作为隐私权的客体,而在现实世界中则不是如此。如在现实世界中,性别为一目了然的外观显示,透露某人的真实性别,并不构成对其隐私权的侵犯。而在网络世界中,性别是属于可识别的信息,即属于隐私权的客体。所以,二者的客体内容范围并不完全一致。

(3) 网络与电子商务中个人数据隐私权的客体体现出比传统隐私权更大的经济价值。在网络中,个人资料的价值一方面表现为它是各网站赖以维系的根基,正如一个没人光顾的商店注定要关闭,一个没有相对稳定的网民的网站是维持不长久的。另一方面,对各种从事盈利活动的组织而言,掌握数以万计的个人信息无疑是其盈利的有利条件,通过对这些数据的分析,把握消费者的爱好,预测市场需求,从而及时调整自己的生产和销售计划。据报道,美国一些经营不善的网络公司正计划出售网站所登记的用户资料,价格颇为不菲,一个用户的资料价值10—50美元不等。⁷因此在互联网和电子商务中最有价值的是个人数据,它不仅可以为信息的提供者带来经济利益,而且还是网络信息资料使用者获得巨大经济利益的重要资源。

(4) 二者客体被侵害时,所使用的手段及所造成的后果不同。对传统隐私权的侵害,不需要特别的技术手段就能达到目的。而对网络与电子商务中个人数据隐私权客体的侵害手法,则日趋技术化,所以,在网络与电子商务中,对于个人数据的隐私是防不胜防。随着人类基因工程的进步,有可能将个人资料经过类似于分析基因的做法,从而掌握个人消费特征、性格爱好等。而且,由于互联网无国界,所以,在网络与电子商务中一旦公布个人隐私,其传播范围是传统媒体无法比拟的,所造成的影响是难以消除的。当然,对个人数据隐私权的保护最关键的还不是计算机技术,而是政府如何通过技术政策和法律政策的制定既能恰当地维护社会公众的某些利益,使人们享受物质文明的巨大成果,同时也能兼顾公民个人对自身隐私权的保护、防止他人非法侵害。

⁷参见《破产网络公司最后一招:卖用户资料牟利》转引自《网络侵权行为法》,屈志辉编。

3、关于二者权能的比较。由于二者隐私权的客体处于不同的环境中,所以关于二者隐私权权能也必然不完全相同。传统的隐私权理论往往认为是一种不全面的权利,甚至有人认为它只是一种消极的权利。而网络与电子商务中个人数据隐私已被储存在各种各样的电脑中,相应的隐私权的权能就必须有所变化。网络与电子商务中的隐私权应当是一种全面能动的权利。

⁸熊进克《网络时代与隐私权的法律保护》,载《江西社会科学》2000年第10期

第二章、各国在电子商务时代的个人数据隐私权保

护立法之比较分析

许多国际和区域性组织早已关注个人用户数据隐私权问题，并纷纷开始行动。1996年3月11日，《欧洲议会与欧盟理事会关于数据库法律保护的信息》颁布，要求成员国在1998年1月1日前通过国内立法，将信息的内容贯彻到国内，国际标准化组织（ISO）消费者政策咨询委员会提出有关国际个人隐私（数据）标准的建议，并准备制定以IT为基础的适用于电子商务的个人隐私（数据）国际标准，另设一个技术委员会来负责有关个人隐私的业务。国际电信联盟（ITU）制定了多媒体终端个人隐私（数据）保护技术的标准，还要进一步制定包括隐私问题在内的有关电子商务方面的标准。万国邮政联盟（UPU）制定了与加密和认证问题有关的消费者个人数据的全球政策框架。其中，欧盟的《数据保护指令》最具代表性。

（一）欧盟

1995年10月24日欧盟部长会议通过了《欧盟数据保护指令》（EU Data Protection Directive），于三年后正式施行。1996年9月12日，欧盟理事会通过《电子通讯数据保护指令》，对《数据保护指令》进行补充。1998年10月，欧盟制定的有关电子商务的《私有数据保密法》开始生效，这项法规也是对1995年指令的延续。1999年初，欧盟委员会制定了《互联网上个人隐私权保护的一般原则》，随后又颁布了《关于互联网上软件、硬件进行的不可见的和自动化的个人数据处理的建议》。1999年初，欧盟部长级会议提出《信息高速公路上个人数据收集、处理过程中个人权利保护指南》。考虑到各成员国个人数据保护水平不一，欧盟订立指令以在各国统一的基础上达到和谐。

指令的一大特色是把被保护数据的范围扩大到包括手动数据在内。指令有两个基本目的：一是保障自然人的基本权利和自由，尤其是他们的隐私权；二是确保信息在成员国内自由流动，类似于货物和服务流动的一般原则⁹。欧盟的这部指令规定了数据保护的高级标准，力求消除 15 个成员国之间的数据传输壁垒。指令同时规定，为了使成员国能同欧盟以外的国家进行数据传输，这个国家必须采用同等的保护标准。只有在非欧盟成员国能保证对数据有足够的保护时，欧盟成员国才可以向这些国家传送私人数据。欧盟的这一措施主要是用于保护私人数据，防止一些意外的或非非法的数据破坏，或者意外的数据损失、变更和未经许可的数据曝光或访问，以及其他任何非法形式的操作。根据指令，欧盟与 1998 年宣布禁止美国在线、贝尔、大西洋公司等美国企业横跨大西洋发送消费者的个人数据，引发了美国和欧盟在数据隐私问题上的争论。用户数据的传送在美国是由传送者自己管理的；而在欧盟国家中，如果传送者违反数据保护法律将会被处以罚款。2001 年夏天，欧盟与美国曾达成一个“安全港”协议¹⁰，这一协议用于管理欧盟与美国之间数据的传送范围。关于如何对私人数据提供欧盟数据保护指令中所要求的“足够的保护”，这一协议也为美国的公司组织提供了一个指导。但到目前为止，只有为数不多的公司组织签约遵守这一协议。

指令约束公司收集、组织、储存、采用、篡改、咨询、或泄露欧洲人的个人资料，即约束任何有关“处理资料”的行为。根据指令，数据控制者有两项义务：

1、确保数据质量。根据第 6 条的规定，一个数据的控制者，必须确保个人数据是在公平合理的情况下处理的。指令规定了一些原则来监管数据质量，这些原则控制信息获得的方式和可以获得的数据的类型。原则要求数据控制者：有收集数据的合法目的并作出解释，只收集与该目的有关的数据，只保留为达到这个目的所必须的数据，保

⁹ Article 1 of EU Data Protection Directive

¹⁰ 美国企业必须遵守以下“安全港隐私权原则”，以证明其符合欧盟的数据保护指令：告知、选择、安全、完整、访问和执行。

证数据新且准确，提供适当的安全措施保护数据，允许个人访问他们自己的数据并改正错误的数，告诉个人数据收集者的情况、收集数据的目的和将来会接受数据的第三方的情况，解释个人必须或可以（选择性的）提供数据和如果不提供数据对其的后果。

2、依合法程序处理数据。根据第 7 条的规定，数据的处理必须经数据主体的明示同意；数据管理人为法定义务人，必须保证数据主体的权益；出于公共利益的目的，数据管理者或收集者收集、使用、披露和保留个人数据，仅限于为机构确认的目的所必需，而且方式必须合法公平。指令列举了正当收集数据的几种情形：允许个人选择是否愿意让别人收集或使用其数据，处理个人数据必须有其明确的允许。

（二）美国

对于网络隐私保护问题，美国政府主张自律，克林顿政府提出的首要原则是“私营部门应起主导作用”，强调支持私营企业所采取的自我规范措施。美国没有单独的保密法可以解释一个人何时有权对信息保密。少数联邦法律要求公司对某些东西保密，如信用报告和税单。另外，大多数州有普通的保密法以及涉及某些医疗和财务信息的法律。¹¹唯一一部保护在线隐私权的立法是国会于 1998 年 10 月通过的《儿童在线隐私保护法》（the Child Online Privacy Protection Act），该法规定商业网站收集年龄在 13 岁以下少年的个人信息以及这些未成年少年进入网上聊天室或主动提供自己的个人情况必须首先得到其父母的同意。许多组织都在看这部法律实施的效果，以决定是否要求政府采取立法的形式保护网上隐私权。然而，此法才一出台，便遭指责。批评家指出，这项法律不仅在间接地鼓励孩子隐瞒自己的年龄，而且会造成网站经营成本大幅上升，¹²给商业网站的经营增加了沉重的负担。于是，国会在立法上陷入了尴尬的境地，内部也分裂成

¹¹（美）苏珊·巴特勒著：《电子商务法律手册》，张建珍、梁慧社、张友联、于薇译，企业管理出版社 2001 年 5 月版，第 317 页。

¹²专家预计，一个网站要完全做到符合这项法律的规定，仅支付额外聘请的管理登记系统的员工工资一项，每年就必须增加 6 万到 10 万美国的经营成本预算。

两派，分别支持自律和立法，前者占据了上风。因为，美国是世界上电子商务发展最快的国家，而立法有可能阻碍电子商务的发展。

早在 1995 年起，联邦贸易委员会（the Federal Trade Commission, 以下简称 FTC）就着手研究在线隐私权问题的解决之道并鼓励实施自律。1997—1999 年度，FTC 作出互联网上用户隐私保护的相关报告，报告提出信息保护的五大原则：（1）通知/知悉原则（the notice/awareness principle），这是核心原则，要求信息收集者在收集用户信息前告知用户何种信息将被收集以及信息的使用目的。（2）访问/参与原则（the access/participation principle），要求信息收集者提供合理的途径，允许用户访问其被收集的个人信息，审查信息的准确性与完整性，对不实数据享有修改权。（3）选择/同意原则（the choice/consent principle），要求信息收集者提供给用户选择权，让用户自行决定是否允许被收集的信息被使用及如何使用。（4）完整/安全原则（the integrity/security principle）要求信息收集者采取合理措施确保收集到的信息的完整和安全。（5）强制执行/救济原则（the enforcement/redress principle），要求制裁不遵从公平信息准则的行为。

13

1、业界自律。美国的业界旗帜鲜明地主张以自律方式来保护个人可识别数据信息，一些私营企业团体发布指导方针指引集团成员在收集用户个人数据信息时保护其隐私权。

（1）银行业：银行家圆桌会议为银行实施隐私权原则制定了详尽的方针。该方针包括：①了解用户对隐私权保护的期望值，即金融机构应尊重用户对隐私权保护的期望值并向用户解释银行的隐私权保护原则；②用户信息的使用、收集和维持，即金融机构收维持和使用个人可识别数据信息只应服务于银行业务和为用户提供产品及服务的目的；③维持信息的精确性；即要求建立确保用户信息正确和最新的程序；④限制员工获取信息，即只有因业务关系需要使用个人可识别数据的员工可以获取这些数据信息；⑤通过设立安全程序保护信

¹³ Major R.Pippin.Consumer Privacy on the Internet:It's "Sufer Beware" .47.A.F.L Rev.125

息，即要求金融机构设立安全标准和程序，禁止未经授权获取用户个人的可识别信息；⑥限制泄露帐户资料，即金融机构不得为了独立第三方的独立使用而向他泄露用户的个人可识别数据信息，除非法律另有规定或经用户同意；⑦在银行与第三方的业务往来中保护用户隐私，即金融机构应要求获得用户个人可识别信息的第三方遵守行业隐私原则；⑧告知用户银行的隐私保护原则，即金融机构应使用户了解银行的隐私保护政策。此外，该方针还要求银行设立一套内部机制，监督银行的行为以确保其遵守方针，处理违规行为，维持用户信息的准确。尽管该方针提到了 FTC 五大原则，却未能像 FTC 一样规定统一的执行程序，而是依赖于各银行内部程序。¹⁴

(2)DMA(the Direct Marketing Association): DMA 也为其成员提供了在线隐私保护准则和信息规范指引。DMA 要求网站经营者收集用户信息时履行告知义务，且使用户有机会阻止其信息被披露。不过 DMA 的准则并未完全遵循 FTC 倡导的五大原则，如在获取个人信息和确保信息安全、准确等方面。此外，若发生违规行为，DMA 准则也不能提供强制执行机制。

(3) IRSG(the Individual Reference Services Group): IRSG 在此方面亦不甘落后，也推出了自己的行业准则。其内容包括：①教育(education),IRSG 要求其成员通过教育手段使公众了解 IRSG 的隐私保护政策以及信息自由流动的益处；②从规范来源获取信息(acquisition of information from reputable sources), 建议成员仅从政府和私营部门这些规范来源获取个人可识别数据信息；③准确(accuracy), IRSG 的成员应当采取一切合理的措施确保个人可识别信息的准确；④安全(security), IRSG 要求成员维护系统，防止他人未经授权获取存储信息；⑤公开(openness), IRSG 的成员应通过网址、广告或教育手段告知用户 IRSG 收集信息所遵循的准则；⑥选择(choice), IRSG 要求成员必须应用户要求为其提供方法限制使用或披露其个人可识别数据信息；⑦访问(access), 应用户要求允许他们访

¹⁴ Jonathan P.Cody.Protecting Privacy over the Internet:Has the Time Come to Abandon Self-Regulation; 48 Cath.U.L.Rev.1183

问自身信息的行为由成员自己掌控。¹⁵不过令人遗憾的是，作为自律体制，IRSG 准则同样缺乏行之有效的强制执行机制。

(4) ISA(the Interactive Services Association): ISA 为在线操作人员和在线服务提供商提供了收集在线信息的准则。ISA 准则要求将隐私保护政策置于网站上，易找易读，便于理解。准则应说明信息正被收集，收集的方法，收集的目的，用户限制披露其个人可识别数据信息的方法。此外，若互联网或在线服务提供商出于商业目的想将信息披露给第三方，用户有权决定是否同意，这样 ISA 成员要将用户资料给第三方就必须征得用户的同意。ISA 准则的弱点在于不能为在线用户提供他们的信息，无法使用户获得任何安全保障，最糟的一点是它同样具有上述三准则的弊端——没有强制执行机制。

2、第三方认证。相对于自律而言，第三方的认证更有利于建立公众的信任，而且认证还可以反过来促进自律的实施。一般来说，所谓“认证”，是由商业网站向第三方机构申请，通过该机构的网站隐私保护合格认证后，得以加入该机构，并可以获得这一机构颁发的易识别的徽章或记号，通常这种方式也被称为“保护程度标志化”。商业网站获得的徽章或记号是一种信息标志，本身不具有法律效力，只是用以向公众表明该网站保护用户隐私的态度，以提高用户对公司的信任程度并且塑造其良好形象。

(1) TRUSTe Program. TRUSTe 是由电子前线基金会和加利福尼亚州的 CommerceNET 创办的，不以盈利为目的，其主要业务之一是专门制作标签和证书。TRUSTe 的赞助商和合伙人包括微软、IBM、AT&T、康柏等大公司，Coopers&Lybrand 和 KPMG 这两家著名的会计公司帮助它设计方案和查验各网站上的隐私权声明，这样无形之中为 TRUSTe 增添了信誉度。TRUSTe 通过监督来保证其成员遵循它所主张的隐私政策。Trustmarks 是 TRUSTe Program 的核心，它说明某一网站对隐私权问题的做法，允许客户自行选择是否进入某一特定的网站。要获得一个“trustmark”，TRUSTe 的成员必须为访问者

¹⁵ Jonathan P.Cody.supra.

查询、阅读和理解该公司的隐私声明提供方便，告知访问者它已经获得了 TRUSTe 的认证，并且在其隐私声明中说明其信息收集方式。¹⁶此外，成员还应当允许访问者禁止其向第三方传递他们的可识别数据信息。TRUSTe 通过不定期地检查成员的网站来实施监督，以此保证成员遵守他们所声明的隐私保护政策。一经发现某个成员有违规行为，即剥夺该成员使用“trustmark”的权利，将其从 TRUSTe 中扫地出门，并将该网站列入“不守规矩的网站”的名单中，TRUSTe 也无需履行与其签订的协议，必要时甚至可以将其以欺诈罪推上联邦法院，由此向外界证明它拥有强制实施的有效手段。当然，TRUSTe 还有其他的监管措施，比如要求成员提供注册会计师事务所的审计报告，接受网民的反馈和投诉，等等。

(2) BBB Program(BBBOnline Privacy Program)。BBB Program 是由 BBB(the Better Business Bureau)发起的，将徽章 (BBBOnline Privacy Seal) 授予遵守特定隐私保护准则的公司。要得到该徽章，公司必须接受并实施置于公司网站上的隐私保护政策，遵守 BBB 的规则。一个公司要想加入 BBB Program, 必须在网站上披露一份简单易读的隐私保护政策，告知用户：收集信息主体的身份，所收集的信息类型，如何使用收集到的信息。这三者是 BBB Program 要求参与者接受的隐私保护政策中最基本的要素。网站还必须披露：用户对信息享有选择权，即用户有权选择是否同意网站出于商业目的将其个人信息披露给第三方；网站将采取何种措施确保用户可以访问其个人信息，更正错误，以保证用户信息的准确性；网站将如何保护用户信息的安全。

BBB Program 专门建立了争端解决机制，处理用户对参与者的投诉意见。不过，在接受投诉之后和启动争端解决程序之前这段期间，BBB 会尽量鼓励用户和公司自行解决争端。违背其隐私保护政策声明的公司将被取消徽章，公之于众，甚至可能被提交给适当的联邦机构处理。BBB Program 承诺对参与者实行严格的监督，要求参与者至

¹⁶ TRUSTe 要求成员说明：1、收集什么信息；2、谁在收集信息；3、信息的用途；4、信息的共享者；5、访问者对信息收集和使用的选择权；6、保护信息的安全措施；7、访问者是否可以访问和修改信息。

少每年评估一次他们收集和传递信息的准则。

（三）其他国家

发达工业国家早在 20 世纪 60 年代和 70 年代，就将信息中的个人隐私和数据的保护问题提到了议事的日程上。当时，这些国家的公共机构和私人机构采用最新的信息技术处理大量的个人可识别信息，政府对此的反应是制定数据保护法和个人信息法。1973 年瑞典颁布《数据法》，1976 年西德颁布《联邦保护法》，1978 年法国颁布《数据处理·档案与自由法》，1980 年欧盟颁布《关于保护自动化处理过程中个人数据的条例》，1980 年 OECD 发表《关于保护隐私和个人数据跨国流通指导原则》，1982 年加拿大颁布《隐私保护法》，1984 年英国颁布《数据保护法》。这些法律的基本要点为：国家建立的保存个人信息的系统应该向社会公开；个人有权接触和修改与自己有关的数据；收集到的个人数据只能用于公开声明的和合法的目的；除数据当事人同意外，个人数据不能在上述目的范围外披露或与第三方共享；采取适当的保护措施保证个人数据的安全和完整。

加拿大在 1982 年就出台了《联邦隐私保护法》，在公共部门的领域内对个人隐私加以保护。为适应互联网的高速发展，1993 年通过《魁北克 68 号法案：关于私人机构中的个人信息保护法案》，该法适用于私人收集、持有、使用和公开所有个人信息，限制企业采取的有组织的经济活动。个人数据的收集应当经过数据当事人的同意，不得擅自收集、传播、披露、共享个人数据，更不得未经当事人同意进行个人数据的交易。1998 年 10 月 1 日，又针对私营部门的个人隐私保护问题制定了《个人信息保护和电子文件法案》（即《C—54 法案》，以下简称“法案”）》该法案针对机构或组织收集、使用或披露个人信息，赋予加拿大公民对个人隐私保护的权利“。法案适用于：（1）省际、国际或商业活动中收集、使用或披露个人信息的任何组织；（2）收集、使用或者披露与联邦企事业或商业有关联的雇员个人信息的任何组织。在内容方面，法案吸收了加拿大标准协会的《个人信息保护示范法典》，调整私营部门范围内个人隐私的保护问题。

（四）比较分析及启示：

总的来说，世界各国在对待网络个人数据隐私权保护问题上一般采取两种手段：一种是法律手段，以欧盟等世界上大多数国家为代表；另一种就是自律手段，以美国为代表。这两种保护手段虽然在很大程度上能确保网络个人数据隐私权不受侵犯，但是它们各自仍然存在不足之处。

对于法律手段来说，尽管法律具有稳定性、可预见性、普遍性等性质，这些性质和法律的弊端有着不可分割的联系，事物总是有两面性，“有光的地方，就有阴影”，法律同样存在时滞性、僵化性。只有以某种具体的和妥当的方式将刚性与灵活性完美地结合在一起的法律制度，才是真正伟大的法律制度。在这些法律制度的原则、具体制度和技術中，它们把稳定连续性的优点和发展变化的利益联系起来，从而获得了一种在不利的情形下也可以长期存在和避免灾难的能力。¹⁷但是，要建立这样伟大的法律制度，法律文化至少要经过数百年的发展才有可能，因为这对于立法者要求无疑过高，立法者必须洞悉社会的发展趋势，正义的要求，权利的演化等等。欧盟的数据保护指令在具有法的一般弊端的同时，自身还存有一些问题：

1、欧盟指令的适用范围在实践上有很大的不确定性。指令的跨国流动规则是以假设为前提的，即国际间的电子资料总是沿着简捷的、可预测的路线流动。然而，这种假设与电子资料的实际传输路线基本上并不一致。原因在于：（1）互联网是一个巨大的高度组织化的网络，具有所谓的“自我治愈”的功能。信息或表示信息的数据被分割成无数的“邮包”，无论目的地在哪，它们都可以找到最有效的路径来传送。因此，传送路径无法以任何地理上的术语来预测。对某一网站中的信息而言，可能有限制获取的对象，也可能没有限制，大多数网站是没有限制的。当网站通过因特网或电子邮件传递信息时，通常只公布已确认的地址，但信息会通过穿越许多国家的网络来传输，而这些国家除了信息首发国和接收国外，还有其他的国家，这些国家

¹⁷ E·博登海默：《法理学法律哲学与法律方法》，邓正来译，中国政法大学出版社1999年版，第406页。

可能没有提供指令所要求的保护制度。(2) 互联网使得世界上的任何地方都能接受信息, 浏览网页, 信息的发送者或者网站的经营人无法有效地控制信息在何地下载或网页在何地被浏览。通过互联网传递的信息可能会在无效考虑当地是否有完备的数据保护法或有有效的数据保护措施的情况下, 向世界上任何地方发送。另外, 指令所确立的数字化规则只能适用于管理少量的信息流通, 而通过互联网传输的信息量十分庞大, 指令的使用难以想象。

2、指令是规范网络中的个人数据处理的, 互联网总是以惊人的速度发生变化, 这使指令的保守倾向更加明显。指令的具体实施, 将会因行业的不同和技术的发展而发生变化, 法律不能朝令夕改, 指令为个人数据的处理设定了一种权利义务模式, 那么为了自由、安全起见, 就应该尽可能避免对指令进行不断的修改。这要求指令具有普遍实用性并保持技术上的中性, 由于网络及其技术的难以把握, 指令在这方面显然不足。而当指令同因网络的变化而产生的一些社会发展力量相冲突时, 指令就要为它的稳定性付出代价。当冲突演变成巨大的危机时, 指令就可能限于瘫痪状态, 不得不为规范模式的调整让路。

对于美国所采用的自律手段来说, 同样也存在很多弊端。美国的消费者权益保护团体大多支持用立法手段来解决网络中的数据隐私权问题, 他们批评自律这一措施和委员会对这一问题的立场, 认为政府对日益增长的在线隐私权保护缺乏有力的措施。他们经常在报纸上、网上以及其他可利用的传播媒介上发表言论, 积极介入诉讼。实际上, 自律的确不能完全解决问题。联邦政府只有有限的权限监管个人信息的收集和传播, 委员会又无权要求商业企业遵守其发布的信息保护原则。私营部门耗费了巨大精力施行的自律体制, 存在许多自身无法解决的弊端。

1、监管的困难。在整个自律体制中, 监管无疑是个薄弱环节。由于缺乏行之有效的监管体系, 很难知道商业网站是否遵守自律体制所提出的准则要求, 这样, 网站不论是从自身的营销角度出发利用用户信息, 还是将用户数据信息售予第三方, 都可从中渔利而无需为此付出代价。另一方面, 监管不力也使用户无从得知网站对其个人信息

的掌握情况，网站如何使用其个人信息，这种情况下，用户根本无法采取任何方法来保护自己的隐私权。更为严重的是，用户往往还会因为网站所获得的标记（如 trustmark 或是 BBBOnline Privacy Seal）而疏于关注网站对其个人信息的使用情况，从而使行业自律的初衷适得其反。

2、自律准则缺乏强制力。自愿是自律体制的一大特点，正是自愿使得自律体制无法实现在线隐私的大范围保护。实际上，美国只有少数在线团体认可和采用行业自律，自律体制难以纳入所有或是绝大部分商业网站。自愿性更糟的一点在于导致自律准则的无法强制执行。一个缺乏强制力的体制势必是一个不健全的体制，无法保障弱者的权利。不能强制要求商业网站遵循自律准则，必然使得一些商业网站滥用用户个人数据信息从中获利，而且这些网站还会因此获得竞争优势，有可能击败那些遵循自律准则的网站，这种不公平现象反过来又会刺激更多的商业网站滥用用户个人信息，隐私权的保护岌岌可危。

3、自律准则缺乏法律救济体系。法律救济制度是弱者自我保护的一种必须手段。早期的救济方式是私力救济，但是弱者通常无法采用此种方式维护自身权益，随着社会的发展，私力救济的不足逐渐为人们所认识，公力救济产生并成为主要的救济形式。网站违反准则规定时，由于缺乏法律规定，用户无法寻求法律救济，而财力的单薄使得自力救济也不尽可行，这实则意味着网站可以违反自律政策而无需花费任何成本，由此网站遵守自律政策的积极性必然减弱。

4、缺乏统一的隐私保护标准和权威的专门保护隐私的政府机构。美国共有 4 个公平信息准则，是 4 个不同的机构制定的，其中 FTC、IITF(the National Telecommunications and Information Administrative, 美国国家远程通信和信息管理局)和 NTIA(Information Infrastructure Task Force, 美国政府信息基础设施项目组)，是政府机构，OECD(经合发组织)是国际组织。¹⁸ 尽管 4 个准则的规定相类似，但是没有确定采

¹⁸ OECD 指出其 1980 年《保护隐私权和个人数据跨国流动指引》(1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) 中规定的公平信息准则同样适用于线上环境。

用其中的一个作为全国统一的政策指导，势必造成一种混乱局面。再者，联邦政府没有授权给任何一个联邦机构，将保护公民隐私作为机构的唯一职能或任务。不论是 FTC、IITF 还是 NTIA，都没有将全部的资源 and 精力投入到保护互联网上的个人隐私中去，这些联邦机构还有别的任务在身。

5、行业自律准则与公平信息准则有差别，企业实际上未遵守公平信息准则。随着各界对隐私权保护的日益关注，许多企业团体纷纷为其成员制定隐私保护准则，但这些行业准则都与已公布的公平信息准则¹⁹有所不同。目前，美国大部分的行业准则都未涵盖公平信息准则的核心部分，只是鼓励成员为用户提供某种形式的告知和在线选择，并未指导成员如何为用户提供访问途径，更鲜有提及安全问题的。何况准则不具有强制执行力，削弱了准则的效力，成员连准则都未能一丝不苟地遵守，更不要说是公平信息准则了。

6、认证存在问题。表面上看，有 TRUSTe Program 和 BBBOnline 可供网站选择，但许多律师建议网站不要轻易将隐私保护政策置于网站上，因为这样做无异于向用户承诺保护他们的个人信息，公司若违反政策，将因此而背上法律责任。这一情况的出现，源起于 TRC 控诉全美最流行的商业网站之一——GeoCities。FTC 指控该网站在收集和使用在线用户个人可识别数据信息上存在欺诈行为：（1）宣称用户以成员模式登陆的，网站收集到的用户个人可识别信息只用于向成员提供特定广告，但实际上，用户信息被售予第三方；（2）宣称用户以申请模式登陆，网站不会将收集到的“选择性信息”披露给第三方，但事实与此相反；（3）宣称网站通过在线竞赛登陆的模式收集和保存儿童个人可识别信息，但实际上竞赛由第三方操纵，第三方收集、储存了儿童信息。²⁰假如 GeoCities 不将其隐私保护政策粘贴在自己的网站上，FTC 就无权过问其行为。由于 TRUSTe Program 和 BBBOnline Program 是自愿性的计划，网站没有加入的义务，于是各商业网站出于利益考虑，会倾向于不在网站主页上设置隐私保护政策

¹⁹指 OECD、IITF、FTC 和 NTIA 制定的准则。

²⁰ Jonathan P. Cody, *supra*.

的链接。

无论是 TRUSTe 还是 BBBOnline, 都无法做到铁面无私, 一视同仁, 在对待发起人的态度上明显有所不同。用户投诉微软²¹在 Windows98 操作系统中安装了可识别码²², 侵害了用户的隐私权。尽管微软声称运用“识别码”是为了发现盗版行为, 即通过“识别码”来判断一套软件是否被安装在多台电脑上, 但是, “识别码”的安装毕竟引发了其他的问题。TRUSTe 收到用户对微软的投诉后, 决定不审核微软的隐私保护准则。TRUSTe 的倾向性意见是对微软谴责了事, 理由是未在微软的网站上发现违规行为。

早在 20 世纪 60 年代, 联邦法院引用联邦宪法第 4 修正案关于公民自由权的规定, 作为隐私权的立法依据, 在适用上扩大了隐私权的范围; 1965 年, 美国开始适用《人权法案》, 使隐私权成为一般性的宪法权利; 1974 年联邦议会制定了《隐私权法》, 后又制定了一系列有关隐私权的立法,²³美国成为世界上隐私权立法最发达的国家。据此, 美国理应对网络隐私权采取立法保护, 而不是借助于自律, 但是美国这一次却反其道而行, 原因何在? 美利坚民族是崇尚自由的民族, 用自律取代法律, 说是传统文化使然也许可以为人所理解, 不过, 究其本质, 我们可以发现, 更深层次的原因在于大企业在幕后运用雄厚的经济实力左右美国的立法。这一点从美国与欧盟的对峙和妥协中看得尤为明显。在美欧之战中, 美国公司在美国与欧洲的对话与对抗中扮演了重要角色。从 1998 年至 2000 年, 美国政府和公司一直试图通过谈判来寻找一种政府和公司都能接受的方式, 以避免美国被迫对隐私保护作出大动干戈的调整。只有摆脱狭隘的集团利益的驱使, 才能更好地落实保护网络空间隐私权的政策和手段。

自律政策在美国国内也受到质疑。FTC 突破了过去的政策, 认为通过行业实行的自我管理“远远达不到要求”, 于 2000 年 5 月敦促

²¹微软是 TRUSTe 的发起合伙人之一, 曾赞助 10 万美元给 TRUSTe Program

²²所谓“识别码”是指, Windows98 会根据用户电脑的硬件配置自动生成一个代码, 该代码具有全球唯一性, 会在用户不知情的情况下将电脑硬件的使用情况传送到微软的网站上去, 微软公司籍此可以知道用户所有的信息输入输出情况, 即 Windows98 可以自动收集用户电脑中的资料。

²³如《公平信息报告法》(Fair Credit Reporting Act of 1970), 《金融隐私权法》(Right to Financial Privacy Act of 1978), 《联邦有线通讯政策法案》(the Federal Cable Communication Privacy Act of 1986) 等等。

美国国会赋予它新的权力，以便保护消费者在线隐私。FTC 采取这一行动的依据是对机构内部进行的调查结果，经过对 Web 网站随机抽样调查，仅有 20% 的网站达到 FTC 制定的自愿性隐私标准。FTC 让消费者封杀对其个人数据的“二次利用”，既不准进行后续的营销活动，又禁止将其透露给其他机构。同时，要求 Web 网站向消费者提供审查有关他们信息的机会以及纠正或删除这些信息的方法。²⁴ FTC 新的立法要求受到电子商务业界的强烈反对，在线隐私联盟作为一个电子商务产业集团，就明确表示拒绝接受 FTC 的建议。针对 FTC 此举，Amazon、eBay、美国在线以及 Lycos 的 CEO 们立刻向 400 多家同行们发出一封公开信，呼吁从事电子商务的网络公司加强对自身行为的约束，认真对待用户的隐私权问题。很明显，业界不希望美国政府采纳 FTC 的建议。白宫对此也没有给予支持。反对者认为立法可能限制消费者的选择，并对开发进一步的技术解决方案起到抑制作用。

²⁴ 《美 FTC 谋求国会授予其管理网上隐私的新权力》，（计算机世界日报 2000 年 5 月 24 日），at <http://news.easy.com.cn/newsdirect.asp?newsid=200052410480288>, April 1, 2002

第三章、网络上对个人数据隐私权的侵害

(一) 侵害个人数据隐私权之原因与后果的社会学分析

韦伯曾这样定义社会学：社会学是“对社会行动的解释性理解的科学，是对社会行动的过程和结果的因果性解释的科学”。²⁵在他看来，决定社会行动的重要条件之一就是行动者赋予其行动的主观意义；而在主观意义中，行动的目的被列于首位。即使是帕累托在其行为理论中提及的无主观目的、无客观目的的非逻辑行为，人们也还是“往往要找某个动机来为他们的行为辩护”。²⁶具体到侵犯网络个人数据隐私权行为，其功利主义的倾向是非常明显的，即对互联网用户隐私权的侵犯，其根本的动因还是为了获得经济上的收益。社会交换理论的代表人物霍曼斯曾对这种功利主义的倾向作过详尽的分析，他认为人们的行动总是为了追求最大利润，换言之，就是为了获取尽可能多的酬赏和避免尽可能多的惩罚，这在他的理论中分别被称为正价值和负价值。既然存在利润最大的问题，就必然存在不同行为的成本与收益比较。较之传统的商业营销、公司监控和个人创收，采用收集网上个人隐私的方式显然在同等收益或效果的情况下，所花费的成本要低的多。因此这一行为在动机上是很容易被理解的。

不过，霍曼斯也指出人们意欲获得的酬赏不但包括货币和商品，还包括对人们的赞赏、尊重等非物质性的标志。按照他的理论，酬赏给行动者带来的是正价值，只有正价值相对较高时，人们才会选择与之对应的行动方案。可是，靠侵犯网络隐私权获取经济收益在非物质的酬赏方面是不可能获得赞赏与尊重的，那么商业公司和黑客为何又选择了这种行为呢？事实上，这里既有互联网自身特点作用的结果，也有商业公司和黑客在道德方面缺乏自律的原因。虽然靠侵犯互联网

²⁵转引自：刘玉安主编，林聚任副主编，西方社会学史，山东大学出版社，1993年，第256页。

²⁶同上，第223页

用户网络隐私权牟利的行为为公众所反对和厌恶，但人们对它产生反感情绪的前提是确实地知道这种行为的存在。然而，互联网的一个显著特点恰恰就是在其中实施某一行为的始作俑者难以追查，而非正当行为的实施者通常还会刻意伪装或隐匿自己的身份，对于缺少专业互联网技术知识的普通用户而言，一睹他的“庐山真面目”就变得更加不可能了。但是，反过来看，假如商业公司和黑客既具备了侵犯网络隐私权的手段和能力，也确知这样的行为可能给他们带来极具诱惑力的经济收益，可是道德准则告诉他们这样做是有损大多数社会成员的公共利益的，那么在道德约束力足够强大的情况下，他们的自律意识就会指导他们在行为上舍利就义，广大互联网用户也就没有必要为此而忧心忡忡了。不幸的是，这里的道德约束力恰恰非常薄弱，这使得侵犯行为的成本（含非物质的赞赏、尊重等方面的牺牲）与收益相比显得更加微不足道，从而也成为行为实施的重要决定因素。

侵犯网络个人数据隐私权行为得以存在并呈扩散之势的另一原因在于缺少惩治这种行为的有效社会手段。根据霍曼斯判断人们行为的价值命题，某一行为的发出除了获取尽可能多的酬赏外，还要尽可能避免惩罚，当这一行为越有可能带来惩罚时，其发出的可能性也就越小。于是，这里就对非正当行为的控制提出了要求。目前对于侵犯网络个人数据隐私权的行为，虽然已经提出了众多的惩罚措施，但行之有效的却十分少见，尤其是最具威慑力的法律手段在这一方面更是相对落后。当人们发现某种有违社会规范的行为不仅能带来相当丰厚的收益，而且能够避开惩罚时，不但相同的行为会被重复，而且还会引诱他们争相效仿，从而使得侵犯网络隐私权的行为蔓延开来。

可以预见，由于个人的网络隐私权受到侵犯而可能给社会带来的负面影响至少有以下几点：

其一，由于数据信息成为一种商品，而且大多数个人数据只是添加到网站上，而未及时进行删除和更新，那么这些变动不居的数据可能带来许多问题。理查德·A·斯皮内洛在《世纪道德——信息技术的伦理方面》一书中将这些问题概括为四种可能性：

- 把数据出售给不负责任的供应商的可能；

- 数据采集者不可信和不谨慎的可能；
- 数据重组后生成有关个人高度详细的、组合的形象的可能；
- 不准确信息传播到其他文件后，纠正困难的可能。

斯皮内洛还指出，“信息共享所带来的后果远比业界参与者所愿意承认的要广泛和严重的多……消费者们会越来越无法控制有关他们自己的信息，而这些信息以往被认为是保密的。与此同时，由不准确的信息造成的伤害将随着这些数据的自由流动而增加。”²⁷他甚至认为，个人的隐私将逐渐变成一种虚幻而不再是现实了。当然，这种认识与他对个人隐私的理解有关。姑且不论结语的对错，他所指出的四种可能性却是完全存在的。

其二，向互联网中提供的信息越来越少。虽然随着互联网信息来源的激增，可获得的信息也相应增多，但是由于对个人数据合法隐私权的担心，可能使人们在某种程度上产生一种矛盾的信息权利观，即“我们需要所有的信息，但请千万不要要求我们交出我们的信息供大家分享！”伴随这种信息权利观而来的是一种阻力，是信息共享的明显减少。

其三，互联网中不真实信息越来越多。人们在提供个人信息时会尽可能地小心谨慎，但是正因为这样，人们也不再具有参与收集信息的责任感或公民义务感。人们不愿接受调查，不愿受到打扰，不想参与。这种现象使得信息带上了以偏盖全的性质，因为可获得的想法往往只反映了那些愿意提供数据资料的人的观点——这些人常常是畅所欲言的少数人，而不是能代表整个社会的群体。另一方面，在遇到个人的数据隐私可能被泄露的情况下，人们除了不提供有关个人的信息外，在不得已的时候，通常还会选择提供虚假信息。当人们或者不向互联网提供信息，或者只向其提供虚假信息的时候，互联网中既不完整也不真实的信息将会使它所构筑的虚拟社会变成“虚拟社会”。

这些影响不仅会使互联网本身的运行难以为继，在今后社会交往、经济运行、安全保卫、医疗卫生等日益以互联网为纽带的时代，

²⁷理查德·A·斯皮内洛著，刘刚译，《世纪道德：信息技术的伦理方面》，中央翻译出版社，2000年，第175页。

它们所波及的范围还将超出纯物质形式的网络，而扩大到为整个困在“网”中的人类社会。

如同所有其他新技术、新发明一样，互联网可能被用作促进人类发展之正义事业的手段和工具，也可能被“挟持”，为有违伦理道德和人类共同利益的“黑色”目的服务。人类的生存和发展必须以一定的物质基础作为前提，小到个人，大到社会，这种物质基础都是在形形色色的经济活动中积累起来的。利用互联网加速经济发展，加快物质财富的积累，无论在客观效果还是主观目的上都是合乎人类前进的规律的。可能对经济利益的过分追求，却与保护个人数据隐私权之间形成了冲突。人们对电子交易中个人数据安全的担心会大大削弱对电子商务的信任和支持；而由于个人内心安宁与平静受到威胁，人们参与互联网活动的积极性也会大受影响。然而新技术与新发明的出现并非为了自寻一个最终受人摆布的结局。爱因斯坦说过：“科学是一种强有力的工具，怎么用它，究竟是给人类带来幸福，还是带来灾难，全取决于人自己，而不取决于工具。”因此，对待利弊兼具的事物，关键还在于如何趋利弊害。如今在我们身处的网络时代，一些经济活动如电子商务、银行业、保险业等对用户个人信息的要求越来越详尽，企业对于监控雇员在工作时间内无关行为的要求也越来越高。如何在满足大量的个人信息需求与保护个人网络隐私权之间寻求平衡，才是我们面对这一问题时真正需要关注的焦点。

（二）侵害网络个人数据隐私权的主体或途径

侵犯网络个人数据隐私权的行为若以实施主体为依据进行划分，通常可分为两类，一类是个体行为，另一类则是与之相对的集体行为。所谓集体行为，其实并不是说当侵犯网络隐私权的行为发生时有很多实施者在同时“作案”，它主要是与个体行为形成一种对比，而且由于这类集体行为的实施主体多为商业公司，在规模上也与“个体”相对，故而将其归入“集体”阵营。个体行为与之相比就容易理解得多，它是指由黑客所发出的侵犯网络隐私权的行为。黑客往往都是单独行动，以“个体”称呼就理所当然。

1、商业公司

商业公司在组成上颇有些繁杂，就其与网络的关系而言，有具备实体、生产产品的商业公司，他们在采用传统营销模式的同时也在互联网上开展电子商务，如 Intel、IBM；也有无实体的商业公司，他们纯粹只做电子商务，看起来更象个中间商，如标为网络公司典范的亚马逊网上书店；还有不提供商品只提供服务的网上商业公司，如各类商业网站……商业公司搜集个人数据的动机往往非常简单，他们只是想争取更多的客户，节省更多的广告投入，并在可能的情况下使经营风险最小化。比如一家婴儿用品公司通过商店的购物记录查得了某一购买婴儿用品所用的信用卡号码，在互联网上，这一号码很快就被扩大为一幅描述刚迎来初生小宝贝的一对夫妇的图画。这时，这家婴儿用品公司就可以有的放矢的发送宣传资料，而不必再挖空心思做广告，盲目寻找目标顾客了。又比如一家保险公司在未经授权情况下访问了某网站医疗信息系统。它发现在正在申请公司健康保险的人中，有 30 个在遗传上有患癌症的倾向。如果将来每个患者的医疗费用是 30 万元，那么将要为这些患者付出的总费用约为 900 万元。可是保险公司提前了解到了这一点，于是它的经营风险就大大减少了。在以前，并没有人认为个人信息“除直接交易外还有什么价值，然而随着信息的采集、储存、检索、传播更为便捷之后，这种信息便被认为有了些价值，尤其是可以用作市场营销的工具。”²⁸这就是互联网给我们的个人信息所带来的变化。

对于商业公司这种广泛搜集个人数据的行为，公众所持的态度有贬也有褒。身为电脑专家的华盛顿智囊团“卡托研究会”的索尔维格·伯斯坦就认为：个人信息落入商家之手不但没有太大坏处，反而可能带来一定实惠。她曾在一家宠物店买了几条热带鱼回家，由于当时付帐使用的是信用卡，一家热带鱼公司很快便借这条“红线”查到了她的住址。随后公司的产品便源源不断涌来，让她的家一时间变成了纸上热带鱼的天下。索尔维格说：“这些公司只不过是想让你多买

²⁸理查德·A·斯皮内洛著，刘刚译，《世纪道德：信息技术的伦理方面》，中央翻译出版社，2000年，第171页。

点东西”，“这是我们未来经济运行的方式”。²⁹

但是商业公司的做法似乎越来越令人担忧，因为他们逐渐开始使用一些诸如放置间谍软件、雇佣黑客等不光彩的手段。调查发现，在互联网上 100 个最受欢迎的网址中，大约有一半网址曾搜集过访问他们网址的个人用户数据，其中有 23 个能够将信息植入用户的计算机并在用户不知晓的情况下使用这些信息，但没有一个网址将这种擅自闯入行动告知用户³⁰。这种无视消费者自尊的行为使得越来越多原本对网上交易充满热情的人，为了保证个人信息安全而变的怯步不前。

如果说商业公司对网上个人数据的孜孜以求是因为这种新兴的基于互联网的商业运行模式使个人数据有了前所未有的利用价值，那么也正是有人看到了商家对这种利用价值的追逐，以此为对象发展出一个专门搜集、整理、组合和出售个人数据的行业。这时的个人数据本身也成为了商品，买者求其使用价值，卖者求其价值在交易中所带来的物质回报。个人数据的卖者有时是一些专业数据采集公司，也有一些是以此为生的个人。而数据来源可能是网上的公开数据，也可能是采用非法手段，从互联网用户那里盗来的。令人吃惊的是，除了数据采集公司，有的商业网站也会主动将自己从用户那里搜集来的信息出售给第三方，甚至连政府和公益事业部门也参与其中，从中牟利。在这些交易中，与数据直接相关的数据主体常常毫不知情，他们根本就无法在类似情况下控制有关自己的信息，有效保护个人网络隐私权更加无从谈起。例如，医生和药剂师在向病人开出处方的时候，便获得了有关病人的一系列记录，为了可观的经济收入，他们将得到的有关病人的个人信息出售给专门的数据采集公司。数据采集公司为了获得更加完整的个人资料，会再从其他政府机构（如机动车管理部门、税务机关等）或者从某些意欲靠出售个人数据捞取外快的商业公司处买回一些有价值的信息并对其整理和加工，从而形成有关私人健康、财务背景、生活习惯等的真实写照。这不禁让人生出一种被玩弄于股掌之间的感觉：一个非实体的“自己”正被商家们开心地卖来卖去，

²⁹转引自：张彦《计算机犯罪及其社会控制》，南京大学出版社，2000年，第201页。

³⁰《侵犯网上个人隐私权引起关注》参考消息，2001年6月18日

而那个实体的“自己”却被抛到了九霄云外，完全失去了把握“自我”的权利和机会。

这并不是科幻小说中对未来生活的可怕设想，它也不会只出现在大量基本个人信息都要靠计算机管理和互联网传递的西方发达国家，有迹象表明，在我国已出现了类似以个人数据的搜集、整理和传播为主要服务的网站。深圳有一家出售网友电子邮件地址的网站，它在自我推销的电子邮件中这样写道：“我们收集了全球三千四百万个电脑用户（国内四百万用户）、二十万家企业的 E-mail 信箱地址……而这所有的一切您只需支付几十元人民币。以上所有的 E-mail 地址可在我们的网站下载，如果需用 CD-R 光碟交货，请加付由深圳到您所在地的足够邮资。”³¹看来，保护网络隐私权的达摩克利斯之剑真的是时刻都高悬在我们头顶。

2、黑客

黑客的英文名叫做“hacker”。广义的黑客还泛指一切入侵电脑系统的不速之客，它包括无主观恶意的纯粹表现者和居心险恶的窥密者，对互联网用户的个人数据隐私权构成威胁甚至造成侵害的正是后者。早期的黑客主要将攻击目标定与网络或系统的安全防卫体系，他们闯入计算机系统并留下证据的目的只是想让人们知道他们的技术高超，并无意偷走数据或进行破坏。然而随着“黑客”概念的外延不断扩大，互联网中的具体个人数据也成为了黑客所钟情的对象，这时的行为动机就完全是出于金钱的诱惑了。

黑客的生财之道主要有二种：

(1) 进入电子商务公司或金融系统的用户信息数据库，非法假借用户的身份挥霍资财，或是以盗得的用户数据敲诈勒索受侵犯的对象。就在 2002 年，互联网中发生了多起网站被侵袭，信用卡资料失窃的事件。2002 年 3 月 6 日，一位网络安全调查者和被攻击的公司宣称：一名黑客利用微软公司软件的安全漏洞从至少 8 家小型电子商务网站偷走了用户的信用卡号码，总量大约有 350,000 个，对象包

³¹保护我们的 E-mail 地址，available at <http://magazine.shtetl.com/epublish/gb/paper118/8/class011800001/index.htm>

括 yahoo、ebay、加拿大无线电话销售商 Prombility.net、美国 SalesGate.com 公司（它为其他网站提供信用卡记帐服务）、美国网上健康产品销售商 LTA 媒体公司和 Feelgoodfalls.com 公司。另有 4 名少年黑客通过互联网欺骗美国在线和 Earthlink 的用户，取得了这些用户的信用卡帐号信息，并利用骗得的信息在互联网上大肆挥霍他人资财。他们总共购买了价值 8000 美元的商品，然后留下无人居住的房子作为送货地址，以免暴露身份。³²不过，还有些黑客胃口更是大得惊人，他们窃得用户个人数据后不是自己挥霍，而是以此要挟受侵袭的网站进行敲诈勒索，如若要求得不到满足，他们就会撕破脸皮将所得敏感信息在网上广泛散布。2002 年 1 月，一位绰号为 Maxus 的俄罗斯少年解密高手向 InternetNews.com 发出了一封电子邮件，宣称他已破解了由位于美国康涅狄格州的 eUniverse 公司经营的在线音乐商店 CD universe.com 的安全密码和由 CyberCash 公司生产、名为 ICVerify 的常用信用卡处理程序，并从 CD Universe 获得包含 30 多万个用户记录的数据库。他以次要挟 CD Universe 支付其 10 万美元，但是却遭到了拒绝。为报复，Maxus 建立了名为 Maxus Credit Cards Datapipe 的网站，在互联网上恶意散发盗来的用户数据。在他制作的网页上，不仅信用卡号码一目了然，访问者甚至还可以查到信用卡的终止日期、持卡人姓名及地址。截止 2002 年 1 月 9 日早上被迫离线前，Maxus 已偷窃并散发了 25,000 份偷来的信用卡号。³³具有讽刺意味的是，这里的商业公司不再仅仅是个人数据隐私权的侵犯者，他们自己也成为了与网络隐私权受侵犯之相关事件的受害者。

(2) 探得互联网用户的上网帐号，窃取其个人电脑中的敏感数据，并跟踪其网上活动，然后将相关信息转售给商业公司牟利。一般来说，黑客采取的手法主要有两种：一是利用“网络机器人”、“网络蜘蛛”等 E-mail 搜索软件来搜集信息，有的软件还是黑客们自编的，只要硬盘空间足够大，这些软件可以一次处理不限数量的 E-mail 地址。据黑客自己说：“国内类似功能的软件有 20 多个”，“……这种生

³² 《黑客盯上你的钱包——信用卡还安全吗？》科学时报，2002 年 3 月 18 日

³³ 《小心，黑客盯上你的钱包——信用卡还安全吗？》，科学时报，2002 年 3 月 18 日。

意和 114 有些类似，只不过 114 提供的是电话号码，而我们提供的是网上的“门牌号码”——E-mail 地址。³⁴

另一种是借助黑客软件，在用户毫无察觉的情况下将个人数据轻松盗走，这比从橱柜里拿走一件大衣甚至还要来得容易。比如在登陆一些网站，特别是那些提供个人服务（如股票、银行）的网站时，用户往往必须填写一些密码之类的个人信息经过身份验证后才能进入。一些“高明”的黑客正是利用了这个过程，在类似“骗子”的黑客程序的帮助下精心伪造一个登陆页面，抢在真正的登陆页面之前出现，待用户“认真”地写下登陆信息并发送之后，真正的登陆页面才姗姗来迟，而这时用户的秘密已被窃取了。与“骗子”程序不同，“特洛伊木马”则是一种常见的象“间谍”一样的黑客程序（它同时也是一种病毒，传播的途径主要是软件下载操作或电子邮件的收发）。感染了这一程序的个人电脑会在其中自动生成一个.exe 或.com 的引导程序，只要一经引导，“特洛伊木马”就会自动启动，而且一旦上网，黑客就能让它暗中运行一些应用程序，如网上浏览、电子银行业务等，简直无所不包。与之功能相似的还有“冰河”、NetBus、Deepphreat、Subserver 等等。

（三）侵害网络中个人数据隐私权的表现行为

1、非法获取信息

第一、使用 cookies³⁵。可以使用 cookies 记录用户的在线信息，包括用户的登陆时间、使用的浏览器的类型和用户的 IP 地址³⁶，还能追踪用户访问过的网页。用户连接使用 cookies 的网站，网站服务器就会将 cookies 和一个独特的标识符（identifier）³⁷存放在用户的计算

³⁴黑客高价出售网民隐私有下文，相关网站已暂时关闭，available at <http://www.mz.gnet.gd.cn/dmynews/docx/tech-100-10-30-09-19-21.htm>.

³⁵ Cookies 是用户访问过的网站存放在用户硬盘驱动器上的小数据文件，可使服务提供者在下次接网时认证用户的身份，并能够在用户网址上“复制”其看过的内容。暂时的 cookie 没有日期，且当用户推出浏览器时，信息就会被删除，持久性的 cookies 有一个到期日，在该截止日之前通常被存储在用户的硬盘驱动器上。

³⁶ IP 是 Internet Protocol，互联网协议，制定了网络上传送的数据包的资料格式及传送规则。参见薛永生编著：《Internet 应用技术》，厦门大学出版社 1998 年版，第 6 页。IP 地址是指用户的计算机地址。

³⁷标识符是任意性的，通常不包含关于用户的任何信息。

机硬盘驱动器上，下次用户访问该网站，cookies 被传送回网站服务器，服务器能“记得”用户上次访问期间的所作所为。美国南加州大学安妮伯格信息学院和加州大学伯克利新闻研究生院（USC/UCBerkeley）联合组织实施了一项针对数百家媒体网站对用户隐私保护情况的最新调查，该调查表明，有 68% 的媒体网站利用 cookie 文件；追踪访问者在网站的活动情况，绝大多数媒体网站根本没有说明他们利用 cookie 文件的情况，即便是在那些有明确隐私保护条款的网站当中，也有 34% 未予说明他们在利用 cookie 文件。而在利用 cookie 文件的网站当中，又有 82% 的网站不仅自己收集生成 cookie 文件，还采用第三方——如独立的网站分析公司或者追踪广告浏览情况的广告网络公司——提供的 cookie 数据。但是，绝大多数采用了第三方 cookie 数据的网站也没有向用户说明这一情况，即使是在那些用户隐私保护做得相对较好的网站当中，也有一半以上没有说明。³⁸虽然人们对 cookies 的了解逐步得到深入，但 cookies 经常是在用户不知情的情况下设置的，且未经用户允许而使用他们的计算机。首先，许多用户不知道 cookies 的存在。许多网页浏览器处于系统设定状态，并未告知用户已经安了 cookies，用户无从表示反对。其次，即使用户知道 cookies 的存在，要知道如何拒绝设置 cookies 或要求在 cookies 设置之前收到通知，必须花费时间和精力，且比较麻烦。最后，如果用户要求在安装 cookies 之前被告知，他们也难以理解收到的关于 cookies 名称和功用的信息，而选项通常只有“OK”（同意）和“Cancel”（取消），这导致用户在不知情的情况下糊里糊涂点击“OK”（也许用户认为点击“Cancel”将取消他将浏览的页面）。网景和微软在其浏览器的新版本中，虽然都允许用户就是否关闭“cookies”功能做出选择，但缺省设定是保留它们。

Cookies 通常被用来追踪用户的浏览器轨迹或在线购买信息，网站经营者包括广告商收集到用户不愿为他人所知的信息，以此分析用户的兴趣爱好，有时还会将信息售予第三人，而用户却毫不知情。通

³⁸ 《用户隐私：媒体网站诚信有几分？》，at <http://news.enet.com.cn/article/200110/20011010049601-1.xml>. March 29.2003

常网站本身较少需要此类信息，而广告商是大量的信息需求者。但不论是广告商自己还是商业网站运用 Cookies 收集用户信息，都是出于商业目的考虑。在缺乏数据保护规范的国家，由于没有明确将个人数据纳入法律保护范围，Cookies 的使用者对于自己的行为是否违法缺乏一定的认识，或者认识到有侵权的可能性但是乐得“无法可依”，只要确定相关立法，这方面的侵权行为就可以在在一定程度上得到控制；而在个人数据被列为法律保护对象的国家，侵权者明知违法而有意为之，应当严惩不贷。

第二、在免费软件内安插广告。免费软件实际上就是共享软件。共享软件以“满意付费”为原则，用户可以先将软件下载使用，试用满意后，再付钱注册或购买无功能限制、无时间限制的正式版。软件厂商通过这种模式推广他们的产品，消费者可以尽情挑选符合自己需求的软件。但是，有些用户只对试用感兴趣，而不愿意花钱注册，注册的使用者寥寥无几，再加上软件破解工具猖獗，为了追求利润，软件商们又换了种花样，改与广告商合作，在软件内安插一个小广告，当消费者上网并使用这类软件时，软件就会自动链接上广告商的服务器下载广告。消费者只需忍受广告，就可以免费使用功能完整的软件。软件商靠软件里的广告获取收入，而广告商通过广告来了解用户的喜好，从中获利，双方各取所需。此类免费软件，被称为 Adware，我们常用的 FoxMails 就属于这一类。尽管用户可以免费使用软件，但是天下没有白吃的午餐，用户在不花钱享用软件的背后，有可能以付出自己的隐私为代价。因为下载广告的动作通常是在背后执行，用户全然不知，有些 Adware 会自动记录用户上网浏览的习惯，如经常浏览的网站种类等，然后将这些资料传回给广告商，使广告商根据这些资料知悉用户可能感兴趣的广告，拍摄出更具针对性的广告。另外，广告商还有可能将用户的这些资料售予第三方作为商业分析等用途。有的免费软件在安装时会在授权合约中显示软件商和广告商的上述行为，但是用户大多不会仔细阅读合约，便点击“同意”。而在目前，从法律的角度出发，各国对 Adware 似乎都“无计可施”。

第三、使用“木马”。“木马”这种病毒程序，可能使电脑用户的

隐私暴露无遗，尽管“木马”本身不会对电脑本身构成损坏，但它会暗中将用户的私人信息发往其它 IP 地址，使个人隐私受到侵犯。著名电脑病毒防治公司赛门铁克公司曾经报道，Grokster、Limewire 文档共享软件中捆绑的名为“Clicktilluwin”的广告软件内含有一个名为“W32.DIDer”的程序，该程序会自动安装，可被归类为特洛伊木马病毒(Trojan horse)。赛门铁克建议用户在安装文档共享软件之后扫描电脑，确保“W32.DIDer”程序代码被彻底删除。³⁹“木马”使得人心惶惶，用户上网，可以看到在许多大型的网站上都有提醒用户小心“木马”的警示语句。

第四、雇主监视雇员。雇主们监视员工在工作场所的表现早已不是什么新鲜事，监视手段随着科学技术的进步也越来越先进。早期，通常采用闭路电视摄像机、监听装置等。网络时代方法则更加高明，因为计算机是办公必不可少的设备，同时有许多的追踪软件和监视软件可资利用。公司为防止员工利用电子邮件将商业机密向外散布，会监视员工的电子邮件，在这方面，美国有若干个案例⁴⁰。这些案例的法官判定，为保障公司的利益，公司有权对此类电子邮件进行监控。理由是员工在利用公司设备传送电子邮件时，应当认识到公司会对员工在公司内的行为进行管理，因此对隐私权的保护持较低的期望值。美国本属判例法国家，有上述判例为依据，公司更可以恃无忌惮地窥探员工的电子邮件，侵犯员工的隐私权。

据报载，上海已有几十家企业开始使用“网络神探”以制止公费上网及利用企业网络干私活的现象。“网络神探”，指的是一种新开发的“监工”软件，它颇似一位隐身企事业局域网上的“电子工头”，能将每个员工在网络工作站上的所作所为以图像形式记录下来，企事业负责人只要打开浏览器便可一目了然。

第五、政府监控。美国毒品政策办公室在广告中使用了 cookies

³⁹ 《文档共享程序暗藏杀机，内带木马偷窥用户隐私》(Chinabyte2002年1月6日)，at <http://news.easy.com.cn/newsdirect.asp?newsid-2002010611070386838>, March 16,2002

⁴⁰如 Bonita Bourke v.Nissan Motor Corporation in U.S.A.;Alana Shoars v.EPsonAmerica, Inc;Smithv.The Pillsbury ComPany, 参见郭懿美:《论电子商务中的知识产权问题暨解决之道》, at <http://www.civillaw.com.cn/twcivillaw/content.asp?type=法学研究&propramid=1&id=29> July 23,2001

追踪软件。毒品政策办公室在各种各样的站点展示反毒品广告，在搜索引擎中输入和毒品有关的词也会出现反毒品广告，点击这些广告的用户将被带往面向年轻人的毒品政策办公室站点，然后一个 cookie 将置放在用户计算机中。这一事件于 2000 年暴露并受到指责。同年 6 月，白宫命令毒品政策办公室停止通过反毒品广告追踪网络用户。克林顿政府随即发布了关于互联网技术联邦使用的管理法案。白宫管理预算办公室指示所有的机构迅速评估他们是否合乎现有的网络隐私政策，此外各机构秋季要随预算要求递交互联网隐私问题处理报告。⁴¹

“9.11”事件使安全技术成为市场关注的焦点，美国国会以压倒性优势通过了相应法案，授权美国联邦政府对美国境内的数字通信活动进行监控。安全防范措施的加强严重削弱了互联网用户的隐私权，根据美国国会制定的新法律，ISP(网络服务提供商)必须允许政府机构获取通过其网络传送的数据信息。FBI 在 2001 年 12 月份证实，美国政府正在建立另外一种被称为“魔法天窗”的互联网监控系统，以便能更好地对犯罪嫌疑人进行追踪。⁴²这种新技术的出现，对网络用户的隐私无疑构成了巨大的威胁。在收集和使用信息这方面，政府和商业网站的区别在于，前者是公开的且具有强制性，而后者只能在用户同意的前提下为之。

2、不恰当地共享或披露用户信息

并非所有的信息都是通过非法得到的，使用正当的程序往往也能收集到想要的信息。通常有两种方法：

第一，要求用户注册。许多网站通过在线注册、用户提问栏(user profiles)，直接从访问他们的用户那里收集信息。有些网站的网页通常要求用户注册后方能进入。注册要求提供的信息几乎将个人的可识别信息“一网打尽”，包括姓名、性别、出生年月日、住址、电子邮箱、职业、收入等等。上述几个栏目通常是网站要求用户必须填写的，

⁴¹ 《美国政府发布网络隐私指示》(电脑报 2000 年 6 月 24 日)，at

<http://news.easy.com.cn/newsdirect.asp?newsid=20000624165432224>，April 1,2002

⁴² 《并购、病毒、网络隐私：2001 年 IT 业大事记》(新浪科技 2001 年 12 月 20 日)，at

<http://news.easy.com.cn/newsdirect.asp?newsid=2001122015552385537>，March 28,2002

必填的栏目未填,则拒绝用户提交注册表。通过在线注册来收集信息,用户可以自行决定是否将个人信息提交给网站,网站相应地提供一些优惠,诸如允许用户访问全部或部分站点,更新版本、时事通讯等等,以吸引用户注册。直接收集是以明示的方式收集个人信息,从表面上来看,用户事先被告知,并可自由决定是否透露个人信息。但实际上,用户的选择范围过于狭小,以申请电子邮箱为例,用户想要发送 E-mail,就必须使用电子邮箱,而几乎每一个提供邮箱服务的网站都要求用户注册,用户的选择结果不是 A 站就是 B 站。换言之,用户要想享受此类服务,就得提供个人信息作交换。当然,用户也可能提供虚假信息。

第二、查询公用记录。通常是到一些公共网站查询公用记录,从中获取个人信息,然后经过分析比较、整理归类,形成所需信息。许多政府机构或社会团体为了公益的目的,会开设公共网站,存储个人数据,同时允许公众访问。政府信息化建设也使政府将公民的部分登记档案电子化,以备公众查询。公共网站对于来访大多不作限制,且提供的个人数据是经过系统的调查取得,可靠性较高,因此,极易成为个人数据的原始来源地,从而成为别有用心者的利用工具。一些网站专门从公共站点收集个人信息,分门别类进行汇总,然后将之用于其他目的。

不论是否使用正当的方法收集个人信息,个人信息被获取后,都有可能被不当使用,用户将信息提供给网站,善意地相信这些信息只会被用于网站告知的使用目的,但实际上,信息往往被用于其他目的,并有可能售予第三人,一些专门出售个人资料的公司通过各种渠道收集了许多个人信息,而后公开标价出售。在美国,这种公司颇有市场,因而颇有扩展的趋势,目前有影响的公司有 1—800U. S. Search, American Datalink, Discreet Data systems 和 Dig Dirt 等。⁴³个人信息的交易完全是在提供信息的用户不知情的情况下进行的,交易双方出于某种商业目的,违背保护个人隐私权的原则。DoubleClick⁴⁴公司总

⁴³梅绍祺主编:《电子商务法律规范》,清华大学出版社 2000 年版,第 87 页

⁴⁴ Doubleclick 公司是美国一家著名的互联网旗帜广告公司,该公司经常在没有事先通知的情况下对用户的

裁凯文·瑞恩(Kevin Ryan)在其发表的一篇文章中称,DoubleClick 公司的确在保护公民隐私权方面犯了一些错误,因为他们没有及时地向公众通报公司的行为和计划采取的行动。凯文·瑞恩的言论表明,该公司并没有真正认识到他们的错误主要在哪里,而这可能是很多商业公司网站都没有真正认识到的问题。许多商业公司网站都有着与DoubleClick 公司类似的行为,它们并没有对保护个人隐私问题给予太多的注意,而这会加剧互联网用户对网络安全和隐私问题的担心。

(四) 侵害网络中个人数据隐私权是一种可赔偿性损害

从以上的分析中我们可以看到,在网络上对个人数据隐私权侵犯的主体主要是商业公司和黑客,他们大多都是故意的通过各种途径获得用户的个人信息来实现其商业价值,但是这里存在的问题是,是否只要某个主体在网络中故意或者无意识的获取了他人的个人数据信息,就构成对隐私权的侵犯?如果我们认定只要有这种侵权行为的存在,是否就应该都对被侵害者给予赔偿而不管是否造成了财产上的损失?

要回答上面的问题,我们首先要对网络隐私权的客体这个重要概念进行分析。个人数据毫无疑问是网络隐私权的重要客体之一。构成隐私有两个要件:一为“私”,二为“隐”。前者指的是纯粹个人的,与公共利益、群体利益无关的事情,这是隐私的本质所在,后者则是指某个事情,某个信息不为人知的事实状态,比如,当事人不愿这种个人私事让他人知道,否则会对当事人产生各种不利的后果;因此,隐私就是一种与公共利益、群体利益无关的,当事人不愿他人知道或他人不便知道的信息。隐私可以分为三种形态:一是个人数据信息,这就是网络时代无形的隐私;二是个人私事;三是个人领域,为有形的隐私⁴⁵。个人数据信息,如前所述,就是有关个人的一切情报资料

浏览行为进行跟踪,并且收集用户的个人信息,行为引起政府部门的注意。美国联邦贸易委员会和纽约总检察官分别对DoubleClick公司的行为进行了调查。该公司被卷入多起隐私权诉讼案,最终公司不得不宣布放弃“更有针对性地为消费者提供真正有价值的广告信息”这一计划,并承诺以更加积极的态度和更有力的措施保护消费者的隐私。

⁴⁵参见王利明:《人格权法新论》,吉林人民出版社,1994年版。

和资讯，通过这些信息，在网络这个虚拟空间里，我们才能识别出某个人，这也是个人数据的重要价值所在；个人私事，则是有关个人的一些与公共利益无关的活动，比如日常社会生活、交往、夫妻之间的生活、婚外关系以及一切私人不愿意公开的活动和事实；个人领域，则是指个人的隐秘范围，如个人居所、电子信箱、日记等。网络空间隐私权的客体包括了个人数据，但是并不限于这个范围，它还包括个人领域（比如电子邮箱）等。因此，个人数据可以说是网络空间隐私权客体最重要的表现形式，在网上对个人数据的非法采集、利用以及不恰当地共享或披露用户数据信息都构成对网络空间隐私权的侵害。

其次，侵害个人数据隐私权的行为和侵害网上其他人格权的行为既有区别也有联系，甚至有可能构成竞合。比如名誉权是人们对公民或法人的品德才能和其他素质的社会综合评价。⁴⁶而网络侵害名誉权的行为主要包括侮辱、诽谤。网络上的侮辱行为一般是书面侮辱，无论在电子邮件、公告板（bulletin board）、聊天室或网页上闲谈、发表正式言论等都可能构成对他人人格的侮辱。在这种情况下，应认定构成侵害名誉权。但是网上的诽谤行为在随着网络的迅猛发展下，呈现快速增长的势头，它有可能和侵害个人数据隐私权存在竞合。比如网络上诽谤主要是传播不利于受害人名誉的虚伪事实或者以他人传播的虚伪事实为依据进行不利于受害人名誉的不当评论。由于网络上信息流动的高速性，这种虚伪事实可能在几秒钟之内就传播到很广泛的领域内，使他人名誉受损害。但是网上侵害名誉权与侵害个人数据隐私权的最大区别就在于，前者的行为是捏造虚假的事实或不正当评论加以散布，而后者的行为主要是把他人的真实个人信息非法披露或者不恰当的共享。当然它们的后果有可能是一样的，都构成对被害人名誉上的损害，都可以要求损害赔偿。再比如侵害个人数据隐私权与网上侵害肖像权就可能构成竞合。网络是一种多媒体技术，包括文字、画面和声音，可以把信息进行全方位的传播。人们也可以非常容易地从网上下载照片或者把自己或他人的照片扫描到互联网上，这样，网

⁴⁶ 杨立新主编：《具体侵权行为法律界定暨实例评析》（上册），吉林人民出版社1999年版，第120页。

上肖像使用所占比例也越来越高，网上侵害肖像权的行为也日渐突出。网上侵害肖像权的行为，主要是未经本人同意使用他人肖像，比如未经本人同意，在网站上使用并发布与信息内容无关的他人肖像，；或者在网站上刊登未经本人同意拍摄的他人非公共场合中的肖像。非公共场合说明这些照片都含有隐私性，拍摄并刊登其肖像一定要经本人同意。这种网上侵害肖像权的行为同时也构成对个人数据隐私权的侵犯，显然个人的肖像当然是构成识别个人的最重要的数据信息，在网站上未经本人同意就把其肖像非法披露、刊登出来就构成侵犯个人数据隐私权。在这种侵权竞合的情况下，当事人就可以根据自身情况选择最有利于自己的侵权之诉。

再次，网络侵害个人数据隐私权的归责原则应是过错责任原则，一般不适用无过错责任原则。因为一般来说，过错责任原则调整的是一般侵权行为的归责问题，特殊侵权行为的归责问题则主要由无过错责任原则调整。侵害个人数据隐私权的行为是一种侵害精神性人格权的行为，绝大部分为一般侵权行为，在网络中侵害人一般都是为了获得经济利益或其他不法目的而侵害他人的个人隐私权，他们主观上必须具备主观过错或者重大过失的要件，并且需要受害人证明。这种主观上的过错是损害赔偿责任构成的基本要件之一。侵权民事责任的立法宗旨是充分、有效、全面地保护当事人的合法权益，禁止人们以任何方式从事法律所禁止的行为，一旦因加害人的行为造成他人的个人隐私损害，就应当予以恢复和补偿。而不论加害人是出于故意和过失。或许有人会觉得如果也把重大过失认定为这种侵权的构成要件之一，可能侵权法会显得过于严格。确实，侵权行为法只有当它避免了过分苛严的责任时，才能作为有效的、有意义的和公正的赔偿体系运行。它作为一个理性所支配的法律，不能要求一个行为不谨慎的人对他人因其行为所产生的一切损害，都承担赔偿责任⁴⁷。无论是从单个侵权行为人的利益出发，还是为了自身生存的愿望，侵权行为法都必须将那些过于“遥远”的损害从其体系中排除出去。但是那些仅是隐私权

⁴⁷参见《欧洲比较侵权行为法》。[德]Christian von bar 著，张新宝译，法律出版社 2004 年 5 月第 2 版，下册第一部分

受到侵害并没有遭受实际损害的原告到底能够获得多少损害赔偿，则是另外一个问题。我们对上述问题的解答重要的途径在于对损害这一侵权行为法上的核心概念作详细的解释。但是什么是法律意义上的损害，几乎没有一个国家的法典对此作过精确的定义。奥地利民法典第1293条对损害的定义是，损害是指一个人在其财产、权利和人身上遭受的一切不利。“不利”的范围限定在财产、权利和人身之内，它所涉及的就是可赔偿性损害。我们一般把损害分为财产损失和非财产损失，这实际上是最重要的分类方法。典型的人格权客体如：生命、身体的完整性、名誉、尊严、自由和身体的自由权等，对它们的侵害就是一种特殊的侵害形态，通常称为非财产损失。在人格权遭受侵害的情况下，没有一个国家将可赔偿性损害的范围限制在由此导致的财产损失之内，只是各个国家的规定又有差异，比如德国和葡萄牙就规定，只有在人格权受到“严重侵害”的情况下才涉及非财产损失的赔偿问题，这是不正确的，因为如果说在“轻微”或“一般”人格权侵害的情况下对财产损失符合条件的给予赔偿，而对于人格权侵权直接相关的非财产损失却不予赔偿是错误的价值观，这将导致只有“严重”的人格权被侵害才能得到“侵权行为法”的保护，使得人格权被置于与财产权相比很不利的地位。应该肯定的是只要存在人格权客体的侵害事实就给予补偿。因为一方面生命、身体完整性、自由、名誉和隐私被看作是和财产利益相比更高一层的利益，而且还有一些因依附于个人的特性而无法用客观标准加以衡量的其他价值。⁴⁸事实上，个人私生活和隐私获得尊重的权利作为与生具有的人格权，今天已经成为侵权行为法对非物质性人格权保护的核心问题。任何对人格权客体的侵害本身就应该是导致赔偿义务的非财产损失，接受这一点，我们才能对人格利益予以赔偿法上更好的保护。对于侵害网络个人数据隐私权来说，只要故意或者重大过失导致有侵害事实的存在，就应该认定为侵权。但是更重要的是被侵害人能否获得损害赔偿却必须在个案中加以具体化。

⁴⁸同上书，第18页

（五）侵害网络个人数据隐私权的民事责任

网络侵害个人数据隐私权的民事责任，必须具备侵害民事责任的一般构成要件，即侵害行为、损害后果、侵害行为与损害后果的因果关系、加害人的过错。一旦行为人构成网络侵害个人数据隐私权，依照我国民法通则第 120 条第 1 款之规定，必须承担以下民事责任：

1、停止侵害

停止侵害是民法通则规定的首选承担侵权的民事责任方式，当加害人对受害人实施侵权时，受害人得依法请求停止侵害。停止侵害只适用于正在进行的侵权行为民事责任之承担，对已经终止的或尚未实施的侵权行为不适用停止侵害的承担民事责任的方式。对于网络侵害个人数据隐私权而言，受害人对于正在发生的侵害，如加害人正在网上宣扬受害人的隐私，或加害人非法获取受害人的个人资料等，得请求停止侵害。

2、赔礼道歉

赔礼道歉作为承担侵害个人数据隐私权民事责任的一种方式，对于赔礼道歉的方式和场合有特殊的要求。即对于个人数据隐私权受到侵害的受害人的赔礼道歉，一般只能在非公开场合进行。如果在公开场合进行，就可能会在客观上继续公开、披露、宣扬或者传播他人的隐私资料，其结果是，通过加害人承担赔礼道歉的民事责任，非但没有使受害人的精神得到慰抚，反而使其受到进一步的损害；对于侵害网络隐私的一个最重要方面——公民的个人数据隐私资料和信息——而言受害人所关注与要求的主要就是他人不要宣扬、公开或披露其私人信息资料，所以赔礼道歉作为承担民事责任的一种方式，一定要慎重适用，一般不能公开进行。

3、赔偿损失

赔偿损失是网络侵害个人数据隐私权应当承担的一种最主要的民事责任。纵观各国民法的规定，对于侵害隐私权的行为，一般都以赔偿作为惟一的或主要的承担民事责任的方式。我国侵权行为法也广

泛地规定了赔偿损失这一承担侵权民事责任的方式，虽然我国民法通则没有确认隐私权，但是，我国最高人民法院的司法解释⁴⁹已经规定侵害隐私权的受害人可以要求精神损害赔偿。在审理网络侵害个人数据隐私权案件时，就赔偿的范围而言，应包括两个方面：一是对受害人受到的精神损害应当进行赔偿。精神损害是受害人因加害人的侵害个人数据隐私权的行为而遭受的感情损害。在侵害公民个人隐私的情况下，精神损害包括公民心理上的悲伤、怨恨、忧虑、失望等痛苦的折磨，严重的精神损害还可能出现长期的精神方面的障碍或者疾病。这种表现因人而异。由于受害人的文化程度、思想状况、涵养不同，承受外来刺激的能力大小就不可能一样，在同等条件下，对非法披露个人隐私的反应也就不同。因此，在确定精神损害程度的时候，就不能只考虑受害人对侵害隐私权行为的反应是否强烈，受害人是否把自己内心的痛苦表现出来，还应考虑侵权行为在一般情况下可能给受害人造成的精神痛苦，具体包括：加害人的主观状态、加害行为的情节及手段、行为内容的恶劣程度、影响范围的大小等等。当然只有侵犯自然人隐私权，才有精神损害赔偿；二是对受害人因隐私权受到损害而产生的其他损害的赔偿。这里的其他损失，主要是附带或间接的财产损失，也包括受害人因精神损害随之出现疾病；对疾病的治疗费用，误工工资或者其他收入；受害人为准备诉讼所花费的金钱和时间；受害人为了进行诉讼所花费的律师费用或者其他相关费用。但是，在下列情况下，公开他人的隐私阻却违法性，不构成对个人数据隐私权的侵害：

(1)受害人同意。在受害人同意他人在网上获取自己的资料，或者同意他人将自己的隐私在网上公布等情况下，因为是经过了受害人的许可，所以行为人的行为阻却违法性。但是受害人的同意必须是受害人真实意思的表示，而且行为人的行为不得超过受害人同意的范围。

(2)为了社会公共利益和国家政治利益的需要而公开他人的个人私事。比如，为了侦破网络犯罪，维护网络安全而对他人的网上行为

⁴⁹ 参见最高人民法院 2001 年公布的《关于确定民事侵权精神损害赔偿责任若干问题的解释》。

进行监听，对政府官员的品行在网上评论或公开其财产收入等，均不构成网上侵害隐私权。

(3)意外事故。在网络上因出现了意外的技术故障或其他意外事故，造成个人资料的泄露或造成个人邮箱的破坏等，行为人可以不承担民事责任。因为网络的技术性很强，偶尔会出现线路的故障，设备的失灵，这是人力所不能预见也不能避免的，加之行为人主观上没有任何过错，此时不构成对个人隐私权的侵害。

第四章 我国保护网络中个人数据隐私权的

应对措施

(一) 我国的隐私权保护概况

1、历史与现实状况

中国古代，等级制度森严，统治阶级才有权力和能力保护自己的隐私，寻常平民百姓只有人体、两性等基本的隐私。为保护皇族的秘密，法律规定严密的保护制度，从秦开始设有窥宫者斩的规定，《宋刑统》则规定：诸阑入宫门徒 2 年，阑入御膳所者，流三千里，登高临宫中者，徒一年。至于议论皇室事务者，为大不敬，为“十恶”之一。⁵⁰而最高统治者不仅监督其僚臣，更对普通百姓实施严密的监视。

近现代，受历史传统等因素的影响，个人隐私长期以来没有得到应有的重视，隐私长久以来作为一个贬义词，不见容于普通的社会伦理。从心理上说，人们总是关心自己的隐私，却对他人的隐私充满了好奇。一些人交谈的话题喜好以他人的隐私为主题，侵犯隐私的行为也可以打着“要想人不知，除非己莫为”的保护伞而大行其道，特别是在文化大革命期间，随意侵犯他人隐私达到登峰造极的地步。

20 世纪 80 年代，计算机进入中国，当时的使用范围局限于国家机关、学校、企事业单位，还没有普及到家庭中，随着汉化系统的问世和经济的发展，家用电脑逐渐占据了电脑市场的大部分份额，使用计算机的人越来越多。1994 年互联网商业化之后，网上用户人数持续增长，随之，出现了侵犯用户网络空间隐私的行为。

1996 年 7 月北京市海淀区人民法院开庭审理的北京大学心理学第 1993 级研究生薛燕戈诉同窗张某利用电子邮件冒名拒绝美国密执安大学为原告提供奖学金一案，是我国最早的涉及使用网络侵害他人

⁵⁰杨立新著《论隐私权》，第 606 页。

隐私与姓名权的案件。⁵¹此后我国侵犯网络空间隐私权的相关案例出现的不多，但并不是说我国不存在这种侵权现象，实际上这种现象已经十分严重。没有诉诸法律的原因在于，一方面我国国民保护隐私的意识薄弱，民众缺乏相关的维权意识，另一方面也没有恰当的法律可资依循，用户发现自己网络空间隐私权受到侵犯，或不以为意，或束手无策，当然更多的情况是用户根本不知道隐私受侵。而且由于我国缺乏这方面的法律，有时连侵权者自己都不知侵犯了他人的隐私权。一旦日后出现此类法律纠纷，传统的法律规定显得捉襟见肘，在制定法中没有可资参考的依据，在实务上的操作也缺乏经验，既难以准确判断事实，又难以依法裁断。

2、法律概况

我国大陆地区尚未构筑出完整的隐私权保护法律体系，隐私权的法律基础与环境相当薄弱，隐私权并未成为民法上一项独立的权利。总体而言，我国还没有针对个人隐私保护的法律，在其他的法律法规中的相关规定也很单薄，隐私权保护，尤其是网络空间的隐私权保护，在我国法律界还是一个新的命题。

宪法是国家的根本大法，具有最高的法律效力。我国《宪法》第38条、第39条、第40条分别规定了一般人格权、住宅自由权、通信自由权。这些条文中隐含着对隐私权的认可与保护，虽然没有“隐私权”三字，但是宪法的这些规定可以作为民法中确认和保护隐私权的根据和可遵循的原则。遗憾的是，民法通则并未明确将隐私权纳入保护范围。作为我国民法人格权制度主要渊源的民法通则，于人身权一节中规定了姓名权、名称权、肖像权、名誉权、荣誉权、婚姻自主权等若干权利种类，却无隐私权之规定。《最高人民法院关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见(试行)》第140条将以书面、口头形式宣扬他人隐私的行为，认定为侵害公民名誉权的行为，立法第一次明文提到了“隐私”，不过在该条文中，“隐私”是作为公民名誉权的一种客体而存在。《最高人民法院关于审理名誉权案件若

⁵¹带此案虽经北京海淀区法院以侵犯姓名权判决张向薛道歉并赔偿1.2万元而结案，但笔者认为侵犯的实际是隐私权，这正好说明网络空间隐私权的保护在我国法律上尚无一席之地，处境尴尬。

干问题的解答》第 7 条规定：“对未经他人同意，擅自公布他人的隐私材料或以书面、口头形式宣扬他人名誉，致他人名誉受到损害的，按照侵害他人名誉处理。”隐私权和名誉权是两种不同的人身权利，在一个条文中加以规定显属不当，尽管立法者和司法者已经注意到保护隐私权的必要性，却仍未将公民的隐私权当作一项独立的人身权利。在司法实务上，公民的隐私权受到侵害时，只有名誉受损，才可以寻求法律上的救济，无疑极不利于受害人得到充分的法律保护和救济。直到 2001 年 2 月 26 日，《关于精神损害赔偿的解释》第 1 条规定：“违反社会公共利益、社会公德侵害他人隐私或者其他人格利益，受害人以侵权为由向人民法院起诉请求赔偿精神损害的，人民法院应当依法予以受理。”第一次以法律规范的形式把隐私权作为独立的人格权加以规定，且规定“违反社会公共利益、社会公德侵害他人隐私可以请求精神损害赔偿”，是一次重大突破。《民事诉讼法》第 66 条关于证据保密的规定，《民事诉讼法》第 120 条和《刑事诉讼法》第 152 条关于不公开审理案件的规定，都有对公民隐私权的间接保护。《刑法》第 245 条：“非法搜查他人身体、住宅，或者非法侵入他人住宅的，处三年以下有期徒刑或者拘役。司法工作人员滥用职权，犯前款罪的，从重处罚。”第 252 条：“隐匿、毁弃或者非法开拆他人信件，侵犯公民通信自由权利，情节严重的，处一年以下有期徒刑或者拘役。”第 284 条：“非法使用窃听、窃照专用器材，造成严重后果的，处二年以下有期徒刑、拘役或者管制。”其他法律法规也有零星的规定。《未成年人保护法》第 30 条规定：“任何组织和个人不得披露未成年人的个人隐私。”人民检察院直接受理的《侵犯公民民主权利人身权利和渎职案件立案标准的规定》第 10 条：“非法开拆他人信件、涂改信件内容、或者宣扬他人隐私、侮辱他人人格、破坏他人名誉的，应予立案。”《统计法》第 14 条规定，属于私人、家庭的单项调查资料，非经本人同意，不得泄露。《银行管理暂行条例》规定，国家保护个人储蓄存款，实行为储户保密的原则。

为了规范我国计算机信息网络的发展，有关部门出台了一些规定，提及网络空间隐私权的保护问题。如《计算机信息网络国际联网

《安全保护管理办法》第7条规定：“用户的通信自由和通信秘密受法律保护，任何单位和个人不得违反法律规定，利用国际互联网侵犯用户的通信自由和通信秘密。”《中华人民共和国计算机信息网络国际互联网管理暂行规定实施办法》第18条规定：“用户应当服从接入单位的管理，遵守用户守则；不得擅自进入未经许可的计算机系统，篡改他人信息；不得在网络上散发恶意信息，冒用他人名义发出信息，侵犯他人隐私；不得制造、传播计算机病毒及从事其他侵犯网络 and 他人合法权益的活动。”2000年12月通过的《全国人民代表大会常务委员会关于维护互联网安全的决定》规定：利用互联网侮辱他人或捏造事实诽谤他人及非法截获、篡改、删除他人的电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密的，可以构成犯罪，依法追究刑事责任。⁵²但是，这些针对互联网新颁布的法规，基本上是从保护国家安全和社会稳定的角度出发制定的，对公民隐私权保护只是一笔带过，无法为网络用户的隐私权提供足够的法律保护。

综上，我国的网络用户既无法求助于传统的隐私权保护制度进行救济，也没有专门的网络隐私保护法规可资依循，对网络空间隐私的保护仅仅限于网站的隐私保护声明，而这些声明大多是包含在网站的整个政策公告之中的，只有屈指可数的几条，且内容过于简单，通常也较少涉及对个人信息的使用说明和相关安全保证，而且还附有许多用词含糊不清的免责条款。面对用户所处的窘境，制定网络空间隐私权保护制度，在我国已经迫在眉睫。

网络空间隐私权保护的框架应以法律法规、行为规范和技术应用为基础。在网络空间隐私权保护模式的选择上，由于我国国情与欧美皆不同，不能生搬硬套他们的方法，宜结合其中值得参考的因素，为我所用。在欧洲，个人数据被视为个人财产的一部分，隐私权是基本人权之一，大部分欧洲国家较重视隐私权的保障，尤其是个人数据的保障，因此许多欧洲国家都有立法保障个人数据。美国对个人数据的法律保障只集中针对政府机构，⁵³对私营企业如何处理个人信息，则

⁵² 《全国人民代表大会常务委员会关于维护互联网安全的决定》第4条

⁵³ 1974年的《隐私权法》，是美国行政法中保护公民隐私权和了解权的一项重要法律，就政府机构对个人

鼓励行业自律，这是美国小政府、大企业的传统使然。我国不存在历史悠久、信誉卓著的大企业，完全依靠企业自行规范，没有相应的法律法规和政府机关管理，信誉度不够，无法取得人们的信任，换言之，单纯的自律在我国无法行得通。要想使互联网真正成为一个自由的空间，充分保护网络用户的权益，政府对网络的规范化管理必不可少，即由政府制定并执行法规。我国是一个成文法传统的国家，以成文法为主要法律形式的特点在现代中国法律上仍然不会改变。法律是我国保护网络空间隐私权的首选之策。保护网络空间隐私权，单靠政府、企业或是个人难以做到，只有多方面共同努力，才有可能解决问题，把危害或损失降到最低限度。法律与自律并不矛盾，而是相得益彰。因此，建议从我国传统的文化背景和现阶段的人文环境出发，采取以立法为主，自律为辅的保护模式。

（二）完善网络空间个人数据隐私权的立法

互联网是一种便于信息交流和商业往来的高新技术媒介，万维网正在以一种前所未有的方式向全世界提供新的销售机会，激发新的营销潜能，然而这种新技术也带来了发生各种新争端的可能，这种争端很可能是以前人们所意想不到的，有时甚至很难理解。目前互联网正在迅猛发展，还相对处于幼年的时期，各种争端的发生不可避免。但是，使用新技术从事商业活动带来了新的法律上的可能性和不确定性。因为从可能的混乱中必然产生一种新的秩序，产生相应的新法律法规来解决争端。互联网的全球性和匿名性导致了产生一种特别的法律的需要，而随着电子商务活动的来临，更要以法律程序来管理互联网。互联网环境中的法律不应被当作对贸易自由化的不必要约束，而应该是在任何国家得以公平地从事交易活动的惟一保护神。法律对互联网的重要性是不言而喻的，它是互联网得以组织、电子商务活动得以规范、争端得以解决，以及公平和平衡得以实现的机制。

在互联网高速发展的同时，我国的电子商务日新月异。尽管如此，

信息的采集、使用、公开和保密问题作了详细规定，以此规范联邦政府处理个人信息的行为，平衡公共利益和个人隐私权之间的矛盾。

在我国，在 IT 行业之外对互联网几乎一无所知的还大有人在，与互联网交易活动和电子商务活动等法律问题有关的资料很少，仅有的一点法律条文也是近几年才出现的。如果要把互联网这种媒体用于商业目的，那么为确保在万维网上从事商业活动的安全性，就必须发展与此相关的法律体系。互联网已使得现存的法律、法规和实践规范落后于实际的需要，必须推动法律的发展、调整和变动，将法律成功地适用于电子商务活动，以保证商业活动中最小风险和最大获利的可能。

应该说我国政府目前对互联网的监管十分重视，但对于如何监管、监管的力度及如何平衡鼓励扶持与严加管制，把握得尚不到位。亚里士多德曾经说过：“闪耀着人性光辉的法律，将会获得普遍的服从，因其本身是制定良好的法律。”如何制定良好的法律，立法机关重任在肩。网络隐私权的保护需要法律保障，但如果制定法和网络的发展特点不相适应，缺乏可操作性，反而会有损法律的尊严。

1、完善民事立法

民法通则第五章民事权利分为 4 个部分，规定了物权、债权、知识产权和人身权，构成我国民事权利的基本结构，也为撰写制定民法典的格局奠定了基础。我国正在探讨民法典的制定问题，在制定民法典时，宜将隐私权明确纳入人身权的保护范围，确认隐私权为独立的诉因，规定侵害隐私权应承担的民事责任，包括停止侵害、赔礼道歉、赔偿损失、精神损害赔偿等等。法典编纂之初，在概念主义法学理念的支配下，“法典万能论”成为这一时期的支配性思想，认为法典是一个封闭的逻辑自足的体系，涵盖了社会生活的全部内容，但是法典不可能对各种特殊细致的案情提出具体的解决方法。随着时间的推移，概念主义法学受到普遍质疑，人们认识到法具有局限性⁵⁴。民法典是民法法律部门的轴心法律规范，作为制定法理性的最高表现形式，多为原则性规定，需要各种专门法加以补充。鉴于网络空间个人数据隐私权保护的复杂性，不能指望单靠一部法典来解决所有的问题。对网络隐私权的法律保护体现在不同的环节中，包括禁止未经许

⁵⁴法律的局限性表现为法律的不合目的性、不周延性、模糊性、滞后性等等。

可收集、使用用户个人信息，规范垃圾邮件，规范网络服务商(ISP)的责任，因此保护网络隐私权可能要多部不同的法律法规共同完成。需要制定个人数据保护法，电子商务中的消费者保护法，网上广告的管理办法，反垃圾电子邮件的规范，网络服务商的经营规范等等，而个人数据保护法则是重中之重。当然，鉴于网络技术的快速发展，法律的制定难以适从，制定专门的数据保护法必须谨慎从事。

2、制定专门的数据保护法

一部完整的数据保护法主要应当包括以下几方面的内容：

(1) 个人数据。个人数据指所有能够帮助识别或间接识别关于自然人个体身份的数据。不论存储体是什么材料(纸、磁盘、碟片、大容量只读存储器，等等)，只要个人数值被安置于某一符合法定的文件概念的整体之中时，便属于法律的调整范围。

(2) 数据收集主体。数据收集者收集个人数据必须事先经过批准，具有合法资格。⁵⁵我国收集数据的主体可以分为两类。(1)国家机关：国家机关出于职能管理和监督的需要，势必要收集用户的个人可识别信息，这种行为可以认定为广义的行政行为。(2)其他团体：这些主体必须经过有关机关的批准或备案，方有资格收集网上的可识别个人信息。对于不以赢利为目的的，要履行备案手续；以赢利为目的的，应当经有关机关的批准。⁵⁶此外，从事新闻、出版、教育、医疗器械等互联网信息服务，依照法律、行政法规以及国家有关规定须经有关主管部门审核同意的，在申请经营许可或者履行备案手续前，应当依法经有关主管部门审核同意。⁵⁷

(3) 收集者的义务。收集者具有如下义务：收集、使用、披露个人数据，应当告知数据所有者，并征得其同意；将个人数据保护的政
策向数据所有者明示；保证数据所有人访问、修正、更新被收集的数据；不得将个人数据用于收集目的以外的其他目的；保证收集到的数据

⁵⁵如英国的《数据保护法》就规定，只有经过登记被批准为数据使用人(或数据使用人兼计算机中心)之后，该人才有权持有个人数据。未经登记者的允许而持有登记者已向数据保护登记处申报保护的数据，或明知或故意持有与上述数据内容相同的个人数据，或不遵从数据保护登记处对于数据保护者所发布命令的行为都属犯罪行为。

⁵⁶ 《互联网信息服务管理办法》第4条

⁵⁷ 《互联网信息服务管理办法》第5条

的正确和安全。国家机关收集和使用数据，也必须在法律规定的职权范围内或者经数据所有者的同意。但是，以下情况除外：有正当理由仅供内部使用的；为了维护国家的安全；为了维护公共利益；为了免除数据所有者生命、身体、自由或财产上的紧急危险；为了学术研究的需要，而又无损数据所有者重大利益的；有利于数据所有者的权益。其他团体或个人在下列情况下收集和使用个人数据，不视为违法：已经公开的信息而且对数据所有者无害的；为了学术研究的需要，且对数据所有者的重大利益无害的。

(4) 数据主体的权利。①知情权。个人有权知道自己的数据被谁收集，被收集的数据类型、数据被收集的用途及数据的共享情况。②查阅权。个人有权查阅自己被收集的资料。香港《个人资料(私隐)条例》第 18 条规定，任何个人或代表一名个人的有关人士，可以要求资料使用者告知他，该使用者是否持有该名个人属于其资料当事人的个人资料；如果该资料使用者持有该等资料，要求该使用者提供一份该等资料的复本。该条第四款进一步解释，就某些个人资料而言，如果某资料使用者不是持有该等资料的，但控制该等资料的使用，而控制的方式禁止实际持有该等资料的另一资料使用者依从(不论是完全依从或是部分依从)关乎该等资料的查阅资料要求，他须当作持有该等资料。③修正、更新和请求删除权。个人可以请求访问数据库中有关本人的数据，有权对本人数据的不实部分进行修正、更新或请求删除。美国《隐私权法》规定，当事人有权查询并要求更正官方机构中有关自己的资料，官方必须在 10 天内答复是否接受请求；个人有权取用已经被公开的资料，对收集数据的私人机构，个人有权接触并对错误的资料要求更正。对于个人数据的不当使用，当事人享有损害赔偿请求权。

(5) 公用记录的特殊保护。国家机关、学校、医疗机构等单位 and 部门由于职能或其他需要，通常保留有大量的个人数据，对这些数据的使用不能等同于一般的个人数据。因此，应当在数据保护法中制定一套补充规则，专门适用于公用记录。

(6) 侵权救济。首先要求侵权人停止侵害。停止侵害是适用于

正在进行的侵权行为的民事责任，受害人对于正在发生的对其隐私权的侵害，可以向侵权人或法院提出停止侵害行为的要求。其次要求侵权人消除影响、恢复名誉。我国的司法界早就将侵害他人隐私的行为归为侵害名誉权的行为，那么适用于名誉权的民事责任，自然也适用于隐私权。当然还需注意，消除影响、恢复名誉是以公开的方式进行的，其内容必须事先经法院审查，以免由于采用此种方式不当反而使受害人遭到进一步的损害。再次是赔礼道歉。由于侵权人的侵权行为给受害人的精神造成损害，应该赔礼道歉，给受害人的心理予以抚慰。最后，侵权人应当赔偿损失。纵观各国民法的规定，对于侵犯隐私权的行为，一般都以赔偿作为唯一的或者主要的民事责任承担方式。⁵⁸我国侵权行为法也规定赔偿损失是承担侵权的民事责任方式，而根据《民法通则》、《最高人民法院关于贯彻执行〈中华人民共和国民法通则〉若干问题的意见(试行)》第140条和《关于精神损害赔偿的解释》第1条的规定，立法者早就认可了赔偿损失是侵犯隐私权应承担的一项民事责任。况且绝大多数网络的建立是出于商业的目的，网络的商业性质，为侵权者承担赔偿责任提供了法理上的依据和经济上的可行性。

⁵⁸ 《德国民法典》第823条(1)规定：因故意或过失不法侵害他人的生命、身体、健康、自由、所有权或者其他权利者，对被害人负赔偿损害的义务。而20世纪50年代后，德国联邦最高法院已将人格尊严和隐私权解释为民法典第823条(1)所规定的“其他权利”。美国《侵权行为法(第二次)重述》第652条H规定，对侵害隐私权的行为适用金钱赔偿的方式，赔偿的范围包括隐私权益、精神损害和其他由法律认可的损害。《瑞士民法典》第28条第1款规定，因不当使用某人的数据而使其人格权受到侵害时，受害人得提出请求制止即将发生的侵害、排除现存的侵害、宣告某项侵害为违法及赔偿。

结束语

以多媒体技术为特征的信息社会在给人类带来繁荣的同时，也给人类长久以来形成的生活模式和价值观念造成冲击，给隐私权的法律保护提出新的挑战。网络最早是在国外出现并普及的，因此对网络带来的问题，外国已先期进行了研究，并采取了保护措施。尽管各国家和地区对用法律还是自律保护网络空间的隐私权，意见不一，在实践中方法不同，但是，都认识到该问题的重要性，并给予了应有的关注和重视。当然，鉴于网络的国际性和无地域性，不考虑国际大环境，单纯地从本国出发制定适用于一国的游戏规则，有可能引发国际争端，美欧之战即为明证。

网络与经济存在明显的互动关系，网络空间隐私权的保护，不仅仅是法律问题，在经济上也具有重大意义。我国正在建设社会主义法治国家，电子商务的发展也方兴未艾，保护网络空间隐私权具有积极和重要意义。不可否认，我国传统道德观念中存在的反对隐私保护的倾向对我国民事立法存在一定的影响，宪法中包含有以保护公民隐私为内容的条文，民法通则却未将相关规定演绎为受民法保护的隐私权。互联网的应用将网络空间的隐私权保护提上了立法的议事日程，但要在原本就薄弱的隐私权保护法律制度下构筑网络空间的隐私权保护制度，似有舍本逐末之嫌，故而，本文提议：先在民法领域建构较完善的隐私权保护制度，再以此制度统领数据保护规范中对网络个人数据隐私权的具体规定，切实维护公民的网络空间隐私权。

参考资料

一、著作类

- 1、[德]克雷斯蒂安·冯·巴尔著：《欧洲比较侵权行为法》下卷，焦美华译，张新宝审校，法律出版社 2004 年 5 月第 2 版。
- 2、张新宝著：《隐私权的法律保护》，群众出版社 1997 年版。
- 3、梅绍祖主编：《电子商务法律规范》，清华大学出版社 2000 年版。
- 4、李德成著：《网络隐私权保护制度初探》，中国方正出版社 2001 年版。
- 5、周忠海主编：《电子商务法导论》，北京邮电大学出版社 2000 年版。
- 6、殷观新、张颖、胡静编著：《电子商务法律热点》，广东科技出版社 2001 年版。
- 7、万以娴著：《论电子商务之法律问题——以网络交易为中心》，法律出版社 2001 年版。
- 8、徐国栋：《民法基本原则解释——成文法局限性之克服》，中国政法大学出版社 1992 年版。
- 9、北京大学法学院人权研究中心编：《司法权利与权利保障》，中国法制出版社 2001 年版。
- 10、杨立新著：《人身权法论》，中国检察出版社 1996 年版。
- 11、王利明、杨立新、姚辉编著：《人格权法》（“九五”规划高等学校法学教材），法律出版社 1997 年版。
- 12、蒋志培主编：《网络与电子商务法》，法律出版社 2001 年版。
- 13、张文显主编：《法理学》（“九五”规划高等学校法学教材），法律出版社 1997 年版。
- 14、夏勇主编：《走向权利的时代》，中国政法大学出版社 2000 年版。
- 15、(美)E·博登海默著：《法理学法律哲学与法律方法》，邓正来译，中国政法大学出版社 1999 年版。
- 16、(美)苏珊·巴特勒著：《电子商务法律手册》，张建珍、梁慧社、张友联、于薇译，企业管理出版社 2001 年版。

- 17、(英)安德鲁·斯帕罗著:《电子商务法律》,林文平、陈耀权译,中国城市出版社 2001 年版。
- 18、John D.R.Craig, Privacy and EmPloyment Law, Hart Publishing, Ltd., 1999.
- 19、James&Michael, Privacy and Human rights:an International and ComParative Study with Special Reference to Developmenis in InformationTechnology , IJNESCO&Dartmouth Publishing ComPany Limited, 1994.

二、资料汇编

- 1、EU Data Protection Directive.
- 2、中国行为法学会新闻侵权研究会编:《计算机、网络法律规范总览》,新华出版社 2001 年第 1 版。

三、论文类

- 1、雷金牛《论网络时代公民隐私权保护》,对外经济贸易大学 2002 年法律硕士学位论文。
- 2、王勇《论美国网络隐私权法律保护的缺陷》,对外经济贸易大学 2002 年法律硕士学位论文。
- 3、范雪融《数据信息隐私权法律保护的比较法研究》,对外经济贸易大学 2002 年硕士学位论文。
- 4、杨静《网络空间隐私权的法律保护》,厦门大学 2001 年硕士学位论文。
- 5、汪丽莉《网络隐私权问题的社会学分析与对策研究》,苏州大学 2001 年硕士学位论文。
- 6、王全弟、赵丽梅:《论网络隐私权的法律保护》,《复旦学报》(社会科学版)2002 年第 1 期。
- 7、谢新洲、李娜:《论网上隐私权的法律保护》,《中国图书馆学报》2000 年第 4 期。
- 8、程远征:《试论个人隐私权在网络中的保护》,《研究生法学》2001 年第 2 期。
- 9、C.贝内特:《加拿大信息高速公路上的个人隐私保护》,《国外社会科学》1997 年第 3 期。

- 10、汤啸天:《网络空间的个人数据与隐私权保护》,《政法论坛》2000年第1期。
- 11、熊进光:《网络时代与隐私权的法律保护》,《江西社会科学》2000年第10期。
- 12、李德成:《论网络隐私权保护制度中的政府行为》,《中国司法》2001年第2期。
- 13、陈洁:《网络隐私权保护急需规范——保护公民网上隐私权的评议》,《科技与法律》2000年第4期。
- 14、刘春燕:《网络时代如何保护个人隐私权》,《天津市政法管理干部学院学报》2001年第2期。
- 15、曹亦萍:《社会信息化与隐私权保护》,《政法论坛》1998年第1期。
- 16、John E Mogg, Data Protection and Privacy:Contents to EuroPean-American Business Council, at <http://210.34.4.2/law>.
- 17、Susan Collins&Masons, the Data Protection Directive, the Computer Law and Security RePort(1995)11 CLSR.
- 18、MajorR.Ken pin, ConsUmer privacy on the Ininternet:It' s surfer Beware, 47 A.E L.Rev.125.
- 19、Jonathan P. Cody, Protecting Privacy overthe Intemet:Has the time come to abandon self regulation?48 Cath.U.L.Rev.1 183.
- 20、LesLie A.Kurtz, The Invisible Becomes Manifest:Information Privacy in a Digital Age, a shbum L.J.151.

四、网站

- 1、 <http://210.34.4.2/law>.
- 2、 <http://210.34.3:8080/index.htm>
- 3、 <http://www.easy.com.cn>
- 4、 <http://www.enet.com.cn>
- 5、 <http://www.pco.org.hk/>

后 记

近年来随着网络的飞速发展，网上侵害隐私权问题已经成为我国社会广泛关注的热点之一。许多媒体都在报道议论该问题，引起我对网络个人数据隐私权的极大兴趣。在导师的指导和支持下，我选择了网络个人数据隐私权方面的研究作为硕士论文的选题。在论文写作过程中当然遇到很多的挑战和困难，但是法学院各位老师总是给予我热情的帮助和鼓励，从选题、理论分析结构到具体叙述方法，无处不包含了导师的谆谆教诲，他博大精深的知识和严谨治学的态度，使我受益匪浅，并将永远督促我今后的工作学习。

同时我要感谢法学院、研究生部老师给予的指导和帮助，对于他们的关心和教导，我表示衷心的感谢。

最后，我要把这篇文献给我的父母，感谢严父慈母的养育之恩，以及他们在经济上和精神上的支持。