硕士学位论文

移动互联网个人信息泄露政府监管研究

Research on Government Regulation of Personal Information Disclosure on Mobile Internet

作　者：王翠莹
导　师：曹明副教授

中国矿业大学
二〇二零年

中图分类号 学校代码 10290

UDC 密 级 公开

中国矿业大学

硕士学位论文

移动互联网个人信息泄露政府监管研究

Research on Government Regulation of Personal Information Disclosure on Mobile Internet

作 者 王翠莹 导 师 曹明副教授

申请学位 管理学硕士 培养单位 公共管理学院

学科专业 公共管理 研究方向 公共安全

答辩委员会主席 祝天智 评 阅 人

致谢

岁月如水，光阴似箭，不经意间时光已从指缝溜走，在中国矿业大学三年的研究生生活即将结束，内心有许许多多的不舍。回想起来，在这三年的时间里，我收获了很多，不仅收获了老师的谆谆教诲、更收获了真挚的同学情、室友情。经过三年的刻苦学习，我不仅掌握了专业知识，也利用闲暇时间学习了自己感兴趣的知识，与此同时社会实践经验也在不断增加。研究生的三年是我学习成长历程中非常珍贵的一段经历，对这段宝贵的人生旅程中结识的老师、同学我都心存感激，感谢你们曾给予我的帮助、鼓励、支持。

首先，我要特别感谢我的导师曹明副教授，感谢曹老师三年来的关心和帮助，从曹老师成为我导师开始，便给予了我无私的关怀和帮助。在学习上，时刻鼓励我学习自己感兴趣的知识，让我逐渐明晰自己毕业以后的工作方向。在生活上，曹老师的关怀更是无微不至，时时刻刻提醒我注意安全，无论何时都让我把安全放在第一位，更不时组织师门活动，为学习的闲暇时刻增添了许多欢乐，让我感受到了师门的温暖。在毕业论文写作时，曹老师在选题、开题报告以及论文的写作、修改和完成都进行了悉心的指导。在论文的写作过程中，遇到难点、疑点向曹老师请教时，曹老师都耐心地进行了指导，在老师的指导下论文思路逐渐清晰起来，毕业论文能够完成离不开老师的的细致与耐心。这份师生情我定当一生铭记，也借此机会真诚的感谢曹老师。

其次，感谢缘分，让我遇到了团结、友爱的室友们。三年的时间，我们从同学变成了朋友，大家一起学习成长。感谢闫兴俊、王静静、赵亚楠等同学们，难忘大家一起泡图书馆学习、一起吃饭聚餐的时光。同时感谢曹门的师姐、师弟、师妹们，在我遇到困难时，你们总能及时给予帮助，在我忙于考试、找工作时，默默地替我做了许多工作，让我能够安心准备考试，谢谢你们。

最后，我必须要感谢我的父亲、母亲，二十多年的求学路离不开你们的支持，每当我遇到困难，遭受挫折时，是你们一直鼓励我、支持我，想到你们一直在我身边，有你们作为我坚强的后盾，我便又拥有了前行的勇气，是你们的爱与鼓励督促我不断成长、不断进步，谢谢你们。

摘　要

当前，我们不管在工作上、学习上还是日常生活上，无时无刻不在享受着移动互联网给我们生活方方面面带来的便利性，使用移动智能终端的用户群体规模的增长迅速已远超 PC 端用户，随着移动互联网技术的不断升级换代，其在我们生活中渗透率必将不断加深，用户群规模也会不断扩大。移动互联网对我们生活的重要性不言而喻，然而其也给我们带来了一系列新问题，总的来说，当前的移动互联网大环境不容乐观。移动智能终端频繁发生泄露用户个人信息的不法行为，给我们的生活增添了不少烦恼，保护移动互联网环境下的用户个人信息已成为全社会关注的焦点问题。政府具有公共管理和公共服务职能，要解决移动互联网发展中同步带来的个人信息泄露问题需要政府发挥相关职能，站在政府监管的角度上，探讨如何使当前的个人信息防护机制更加完善、更有利于实现保护移动互联网环境下个人信息的目标，进而实现在推动移动互联网产业发展的同时，也能为人们创造一个安心的移动互联网空间，使人们能更好地享受移动互联网的便利性。

文章的选题初衷就是探讨移动互联网环境下发生个人信息泄露问题时政府如何监管。文章利用文献分析法、系统分析法、比较分析法等方法进行分析。首先梳理了移动互联网个人信息泄露政府监管的基本概念以及对公共利益理论进行梳理作为本文论述的理论基础。其次，基于系统分析法，建立了政府监管的系统结构图，并在其基础上，总结出了基于监管系统的政府有效监管因素，为下文进一步分析奠定了基础。随后指出了移动互联网个人信息泄露政府监管的现状以及存在的问题，得出存在的问题主要有监管的监管依据不足、监管部门职能冲突、监管过程中责任追究难以及未充分利用行业自律监管等。再次，文章针对总结出的政府监管的有效影响因素进行了详细的分析，寻找政府当前监管工作不利的原因。随后对国外移动互联网个人信息保护的现状进行了比较分析，学习借鉴其长处。最后，文章在前文研究的基础上，基于我国基本国情，提出了优化移动互联网个人信息泄露政府监管的对策，即健全相关法律法规、进一步完善监管机制、强化信息安全教育与宣传的功能、强化行业自律以及加大技术投入，成立高素质监管队伍。笔者希望通过此次研究和分析，可以为推动我国政府更好地保护移动互联网环境下的个人信息提供有价值的参考。

该论文有图 9 幅，表 8 个，参考文献 75 篇。

关键词：移动互联网；个人信息泄露；政府监管；对策

Abstract

At present, we are enjoying the convenience of mobile Internet to all aspects of our life all the time, whether in work, study or daily life, the scale of user group using mobile intelligent terminal has grown rapidly more than that of PC end user. With the upgrading of mobile Internet technology, its penetration rate in our life is bound to deepen, and the scale of user group will continue to expand. The importance of mobile Internet to our life is self-evident, but it also brings us a series of new problems, in general, the current mobile Internet environment is not optimistic. Frequent leakage of mobile intelligent terminals The illegal behavior of personal information has added a lot of troubles to our life, and protecting the personal information of users in the mobile Internet environment has become the focus of the whole society. The government has the functions of public administration and public service. To solve the problem of personal information leakage caused by the development of mobile Internet, the government needs to play the relevant functions. From the perspective of government supervision, this paper discusses how to make the current personal information protection mechanism more perfect and more conducive to the realization of the goal of protecting personal information in the mobile Internet environment, so as to promote the development of mobile Internet industry and create a secure mobile Internet space for people.

The original purpose of this paper is to discuss how the government regulates the disclosure of personal information in the mobile Internet environment. This paper uses the methods of literature analysis, systematic analysis and comparative analysis. Firstly, it combs the basic concept of government supervision and the theory of public interest as the theoretical basis of this thesis. Secondly, based on the system analysis method, the system structure diagram of government supervision is established, and on the basis of it, the effective government supervision factors based on regulatory system are summarized, which lays the foundation for further analysis below. Then it points out the current situation and existing problems of government regulation on the disclosure of personal information on the mobile Internet, and concludes that the existing problems mainly include insufficient regulatory basis, functional conflict of regulatory departments, difficulty in finding the responsibility in the regulatory process, and insufficient use of industry self-regulation. Thirdly, this paper makes a detailed analysis of the effective factors of government regulation summarized, and looks for the reasons for the adverse work of government regulation. Then it makes a

comparative analysis of the current situation of personal information protection in foreign mobile Internet and learns from its advantages. Finally, the article on the basis of above study, based on the basic national conditions in our country, put forward the optimization of the mobile Internet personal information leakage countermeasures of government regulation, namely, improve the relevant laws and regulations, further perfect the supervision mechanism, strengthen the function of the information security education and publicity, strengthening industry self-discipline, and increased investment in technology, set up a high-quality supervision team. The author hopes that this research and analysis can provide valuable reference for the Chinese government to better protect personal information in the mobile Internet environment.

The paper has 9 figures, 8 tables, 75 references.

Keywords: mobile Internet; personal information disclosure; government supervision; countermeasures

目 录

Contents

图清单

表清单

1 绪论

1 Introduction

1.1 研究背景和意义(Research Background and Significance）

1.1.1 研究背景

21 世纪以来，伴随着移动网络通信基础设施的升级换代，我国已经步入互联网与数字经济发展的快车道。我国移动互联网环境下留存的个人信息数据量的发展势头呈现井喷式，取得了一系列创造性的成果。从 2009 年开始，由于时代的进步以及国内技术的发展，国家 3G 网络开始被大规模部署，智能手机出现。2014 年，4G 网络又开始被大规模部署。我国移动互联网的发展伴随着移动通信基础设施的两次升级换代被注入了巨大的能量，掀开了我国移动互联网发展的新篇章。从《中国移动互联网发展报告(2018)》可以看出，中国移动互联网基础设施建设在 2017 年取得了不俗的成绩，4G 网络建设全面铺开，开始 5G 第三阶段试验并着手部署 6G 网络研发。[1]我国移动互联网从无到有，发展速度如此之快，当今社会人们无时无刻不在享受移动互联网的成果，从生活出行、社交活动到医疗健康、教育培训等等。可以说有人活动的地方，就会用到移动互联网。

目前，网络基础设施不断更新换代以及国家提速降费政策的稳步实施，我国移动网民数量再创新高。根据 CNNIC（中国互联网络信息中心）最新发布的《第 42 次中国互联网络发展状况统计报告》显示，截至 2018 年 6 月，互联网普及率达 57.7%，截止 6 月份新增网民数量就达到了 3000 万，网民数量突破 8 亿大关，达到 8.02 亿，较 2017 年末增加 3.8%。其中我国手机网民规模已达到 7.88 亿，截止 6 月份新增手机网民 3509 万人，较 2017 年末增加 4.7%（见图 1-1）。目前我国通过手机上网的互联网用户比例达到 98.3%，比 2017 年底提高 0.8 个百分点（见图 1-2）；使用台式电脑上网的网民比例为 48.9%，比 2017 年底下降了 4.1 个百分点（见图 1-3）。[2]由此可见，移动互联网的发展是当前的趋势，使用移动互联网终端上网的用户数量将持续增长。

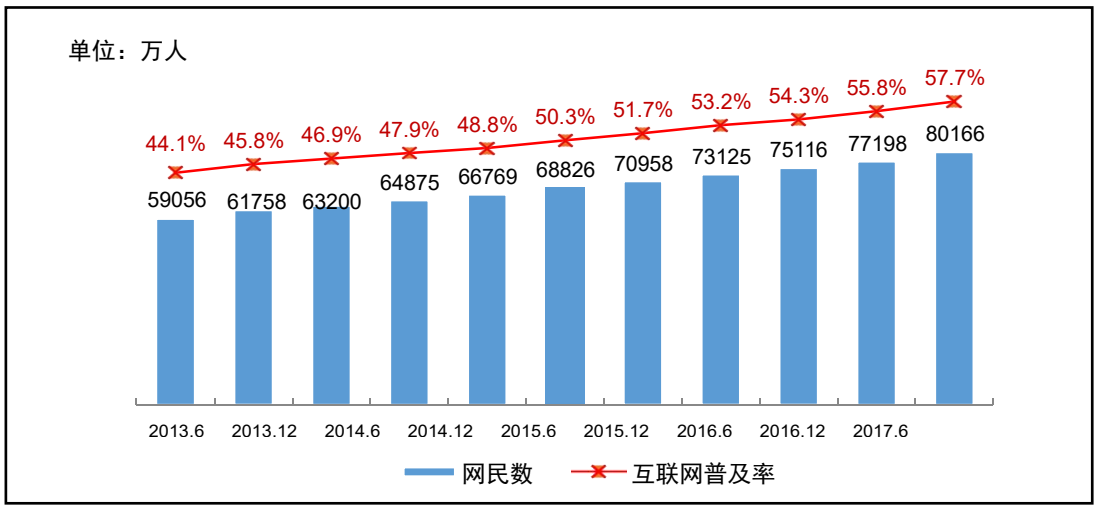

图 1-1 中国网民规模和互联网普及率

Figure 1-1 The size of Chinese internet users and internet penetration rate

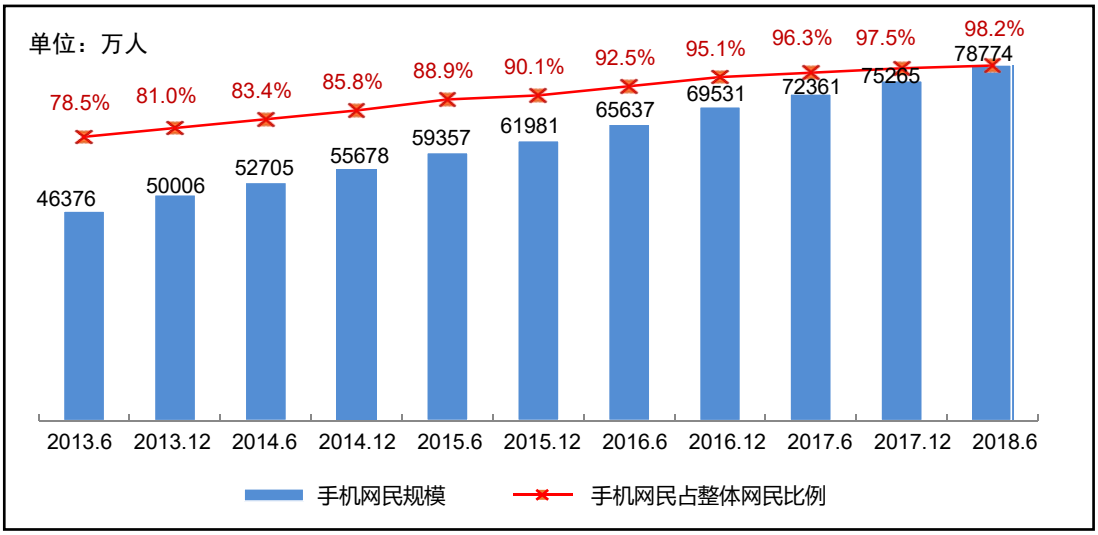

图 1-2 中国手机网民规模及其占网民比例

Figure 1-2 Size and proportion of Chinese mobile internet user

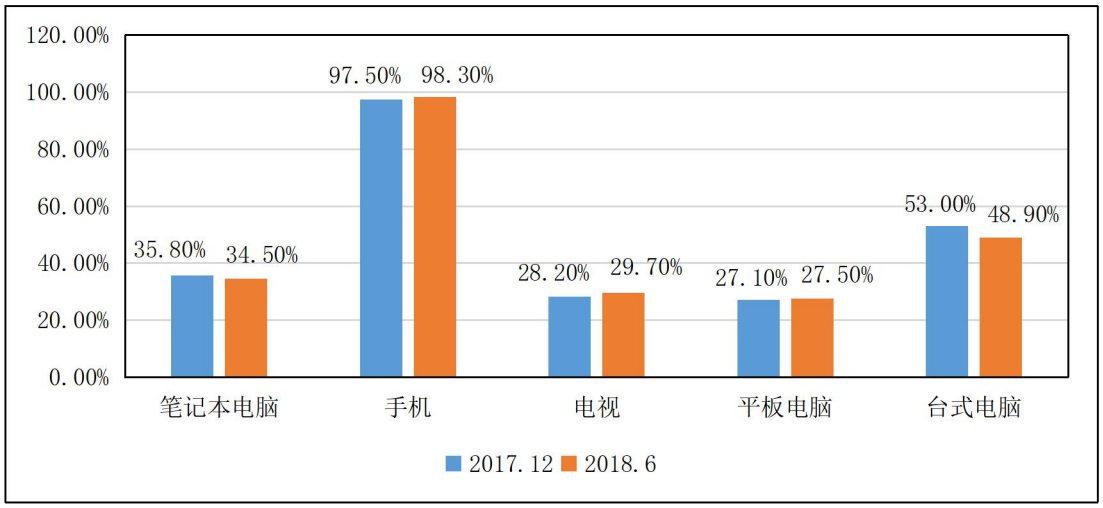

图 1-3 互联网络接入设备使用情况

Figure 1-3 Use of Internet access equipment

面对移动互联网如此高速的发展，我们在体验移动互联网给我们的生活带来便利性的同时，我们也面临着一个很严重的问题：个人信息泄露问题。根据中国青年政治学院互联网法治研究中心和封面智库 2016 年 11 月联合发布的《中国个人信息安全和隐私保护报告》的统计，超过 70%以上的人都认为当前个人信息泄露问题严重（见图 1-4）；接近 81%的人收到过知道自己个人信息（例如姓名和工作单位）的陌生来电；有约 53％的人因搜索网页、浏览网站后将个人信息泄露，不断受到某种广告的骚扰；参与调研者中经历邮箱、即时通讯、微博等网络账号密码被盗的占 40%（见图 1-5）；在使用手机接入 wifi 上网时，参与调研者中有多达 34%的人不会对免费 wifi 进行鉴别后使用，他们只希望确保手机网络时时在线；在确定个人信息被泄露并面临侵害时，相当多的人心存侥幸，他们中的大多数人处理方法比较被动，只有很少一部分人员采取主动对抗的措施。当在解释为什么不能维权的原因时，超过一半的的参与调研者因不知如何维权又或者自身未遭受经济损失而选择了沉默（见图 1-6）。[3]该报告明确揭示了保护个人信息及用户隐私面临的严峻形势。与之前相比，由于移动互联网的迅速普及，我们随时随地都可以看到大批手拿手机的低头族。当前，规模日益庞大的移动互联网终端用户已经成为信息泄露问题的主体，它们已成为各移动运营商数据统计、分析与挖掘的主要研究对象。因为能够从用户的个人信息中获取巨大的经济利益，诱使各种电商平台、组织企业及个人在未经数据信息本人同意的前提下就随意收藏、存储和处理个人信息，随之而来的就是用户个人失去对自身信息的控制，这无疑将给用户个人信息的安全性带来巨大的挑战。那么，在移动互联网普及的今天，确保用户个人信息的安全，使其避免不必要的泄露已经成为亟待解决的问题。

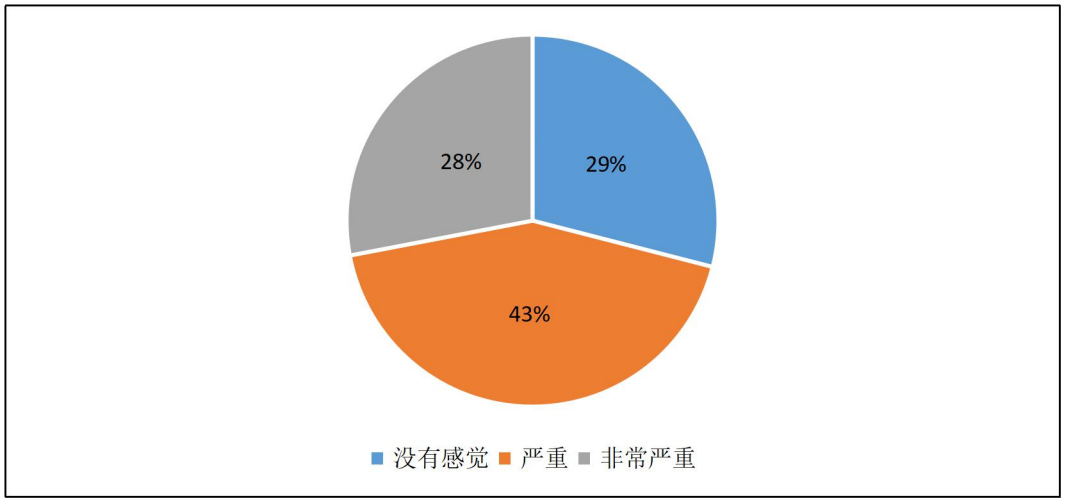

图 1-4 参与调查人群对个人信息泄露问题的整体感受

Figure 1-4 The overall feelings of the people involved in the survey on the problem of personal information disclosure

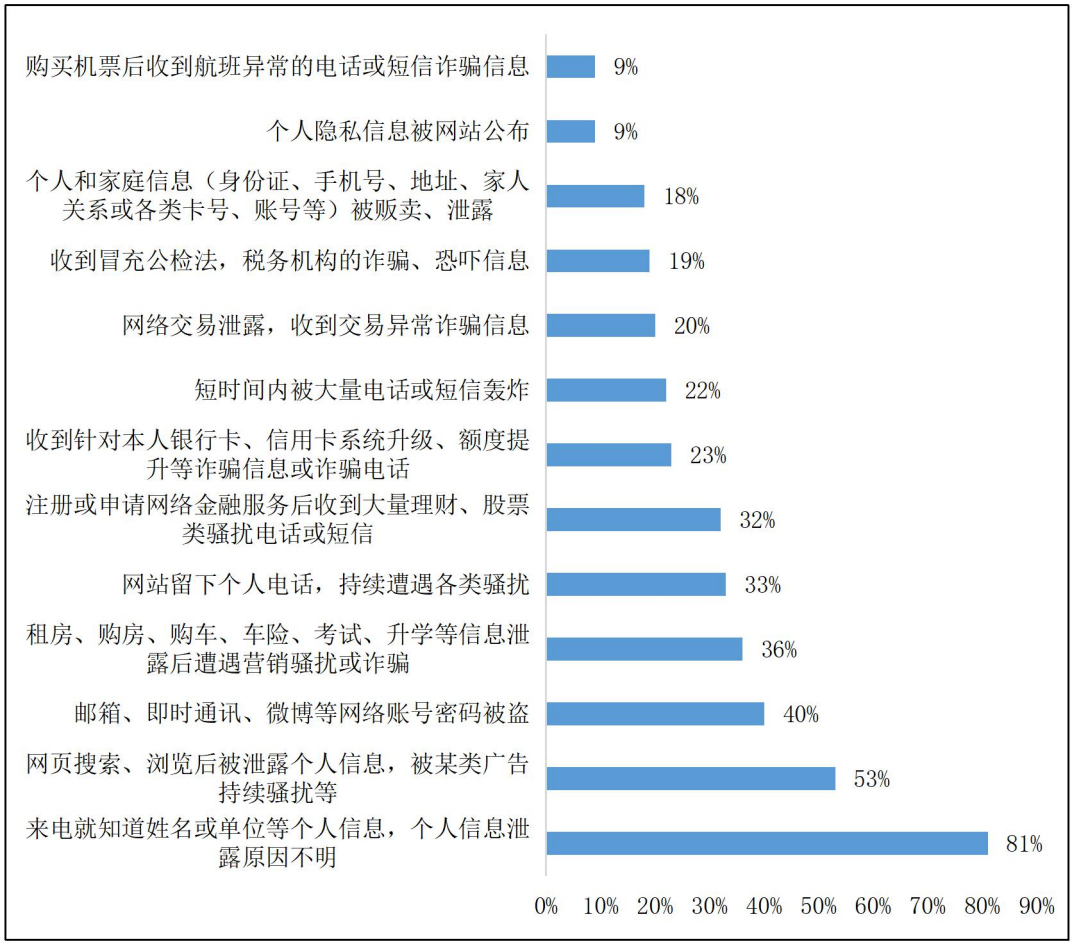

图 1-5 个人信息、隐私受侵害行为调查

Figure 1-5 Investigation into violations of personal information and privacy

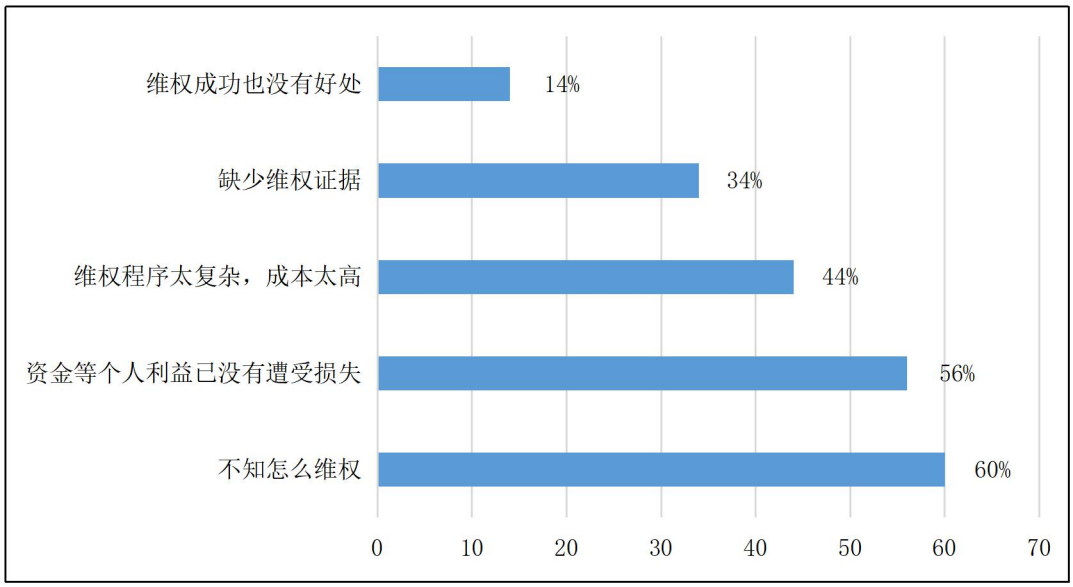

图 1-6 个人信息及隐私受侵害后未能维权的原因

Figure 1-6 Reasons for failure to protect rights after infringement of personal information and privacy

本文正是基于以上背景和研究需要，在了解移动互联网的个人信息泄露严峻形势的基础上，在理解个人信息泄露以及个人信息泄露的概念、特征等相关概念的基础上，总结出影响移动互联网个人信息泄露政府监管的主要因素，并进一步分析当前移动互联网个人信息泄露政府监管的现状和存在的问题，在此过程探讨改进移动互联网环境下个人信息泄露政府监管的对策建议，进而使这场信息技术的新高潮不仅为人们的生活提供便捷同时也能享受安全绿色的环境。

1.1.2 研究意义

（1）理论意义

移动互联网个人信息泄露政府监管研究，首先有利于丰富个人信息保护领域中的研究成果，为完善政府在个人信息保护上的相关理论提供参考。其次，可以丰富和充实我国移动互联网背景下个人信息泄露问题的研究，为建设与移动互联网个人信息监管体制发展相适应的、与互联网发展阶段相协调的移动互联网个人信息监管体系提供了新的落脚点和发展方向。另外，就我国而言，移动互联网环境下，用户个人信息泄露所涉及的的领域在不断扩大，个人信息保护对社会各方面都具有重大意义，移动互联网个人信息泄露政府监管对策的研究，对深化我国移动互联网个人信息监管体系的创新也有着较为重要的理论价值。

（2）实践意义

移动互联网个人信息泄露政府监管研究，一方面，可以提高和促进我国政府对个人信息管理的能力，探索出解决移动互联网环境下个人信息泄露问题的新途径、新方法，以科学合理的理论成果指导具体实践。另一方面，本文研究的意义就在于论题对于当今存在的现状具有很好的指导与改进作用，对移动互联网环境下个人信息泄露问题能进行比较全面客观地分析，对于移动互联网环境下个人信息泄露政府监管的现状、遇到的问题进行分析，进而研究如何从多角度完善移动互联网环境下个人信息泄露政府监管的对策，以期为移动互联网环境下个人信息泄露政府监管提供一定的参考价值。

1.2 国内外研究现状与文献评述（Domestic and International Research Trends and Literature Reviews）

1.2.1 国外研究现状

互联网中个人信息的安全性是不断演变的历史，随着互联网的发展，从网络的诞生开始，网络个人信息安全问题便与之共生共存。在不同的互联网发展阶段，网络功能日益丰富，网络应用不断增多，但随之而来的却是网络个人信息安全问题变得更加复杂化和专业化。在移动互联网高速发展的今天，研究移动互联网环

境下个人信息安全管理问题与对策是热点问题，也是网络长期发展的需要，因而也引起了国内外学者的广泛关注。

(1)关于个人信息概念的研究

国际上，“个人信息”一词在二十世纪七十年代就得到广泛承认，但其概念还未得到统一。“个人数据”、“个人信息”与“个人隐私”是国际社会上关于个人信息的主要法律概念。其中“个人数据”的概念主要被欧盟成员国广泛使用；东亚和俄罗斯等地区使用“个人信息”概念居多；“个人隐私”的概念多被普通法系国家使用，例如：北美和大洋洲等。关于“个人信息”概念的差异实质上并无太大区别，只是形式的不同。Banisar 等人把个人隐私分为以下四类：信息隐私、通信隐私、空间隐私、身体隐私四类。信息隐私主要包括身份证号、银行账号、收入和财产状况、婚姻和家庭成员、医疗档案、消费和需求信息（如购物、买房、车、保险）、网络活动踪迹（如 IP 地址、浏览踪迹、活动内容）等；通信隐私是指个人利用各种通信方式和他人取得联系的过程中形成的信息，主要包括电话、qq、E-mail、微信等；空间隐私，即个人进出的特定空间或区域，包括家庭住址、工作单位以及个人出入的公共场所等；身体隐私，即保护自己身体的安全性，防止侵入性操作，如药物测试等。[4]美国法学家沃伦和布兰戴斯，1890 年在哈佛法学评论第四期上发表的《论隐私权》(The right of privacy)一文中最早提出隐私权的概念，他们提出“个人的私密信息神圣不可侵犯”的法律理念，这一理念确立了“隐私权”这一新权利。[5]在此之后，随着个人数据规模的不断拓展，隐私权的概念变的更加的宽泛。威廉·帕伦特（William Parent）认为隐私权是应当被限定为一种状态，即未成文的个人信息也不能被他人知道或拥有。[6]美国法学家荷尔（William G·Hale）认为隐私权可以定义为每个人的自然权利，即要求自己的私人事务未取得自身同意之前不得公之于众。[7]阿伦·韦斯丁（Alan F·Westin）认为隐私权是：个人、团体或公共机构自主决定何时、如何以及在何种程度上向他人传达自身信息的权利。[8]在此之后，个人信息安全的概念也被提出，特别是在大数据时代，个人信息安全的内容越来越广泛，个人信息数据的量也越来越大，除了个人的姓名、性别、联系方式、居住工作地址等个人基本信息以外，个人信息安全的关键组成部分还包括个人的消费偏好、收入水平、工作性质等潜在的信息。1995 年通过的《欧洲联盟数据保护指令》中指出：“个人信息(个人资料)是指可用来识别自然人(数据主体) 的任何相关信息；可以识别的自然人是指通过身体的、生理的、精神的、经济的、文化的、或身份等的一项或多项信息被直接或间接地识别”。[9]在 2009 年，美国学者 Daniel J.Solove 和 Paul M.Schwartz 主张，个人信息实际上属于一种隐私，实际上是对个人所拥有信息的一种控制，将个人信息归入隐私权进行保护可以界定其权利范围。[10]加拿大《个

人信息保护和电子文件法案》认为个人信息包括所有以书面形式存在和在互联网上存在的个人信息。[11]

（2）关于网络个人信息监管主体研究

针对互联网上存在的问题，Madan Lal Bhasin 认为侵犯隐私是互联网发展过程中一个严重的问题，由于互联网用户拥有完全的隐私权，但各互联网运营主体可以在互联网上收集大量的个人数据，并且随着全球化进程的影响，全球各地的互联网用户都对日益增多的侵犯隐私行为表示担忧。鉴于侵犯个人信息问题的出现，相应政府部门需要转变职能并加大监管力度，处理的不及时、处理方法不合理都可能加剧问题。[12]David Dunbar，Michael Proeve，Rachel Roberts 指出互联网侵犯个人信息问题是一个日益严重的公共卫生问题，需要政府之力。尽管学术界对互联网的研究方兴未艾，但仍有一些问题没有得到很好的解决，仍然需要对互联网进行更多的研究。[13]国外有众多学者认为在针对互联网的治理过程中，政府起到了重要的作用，Carey Doberstein 指出网络监管需要一些基本规则作为依据，才能使监管机制有效运作，而国家是最合适的调解人，国家理应是监管制度设计、执行者，这是多数人的共同观点。[14]

（3）关于保护个人信息方式的研究

一是科学技术手段。为了应对用户位置隐私的不同层次，Ardagna 等人提出了一种利用传感技术对测量到的位置信息进行模糊处理以保护用户位置隐私的解决方案。[15]Bansal 等人指出要保护个人信息必须在所有的声明和法律中明确规定：要合法公平获取；只用作最初获取时已经告知的用途；适当的、相关的并且不过度地使用；信息是准确和最新的；对主体是可访问的；确保信息安全性；完成相关用途后删除。[16]Perlman 最先提出了一种数据可信删除方法，这种方法在基于时间的基础上，可以在预定的时间后被安全删除并永久不能被访问。[17]

二是法律手段。Bauman 指出 2008 年美国颁布的《梅根·梅尔网络欺凌预防法》，这是美国为了应对网络欺凌问题而专门制订的，条文中详细规定了，对犯网络欺凌的人将面临应用刑法中的骚扰罪来处罚，他们将会被罚款或被监禁（最多两年），处罚也可能会视欺凌程度而变动。[18]Helen Dixon 等学者指出为了防止有意或无意滥用个人信息，欧盟出台了《一般数据保护条例》，本法的创新之处在于构建了问责制的基本原则，大大的保护了个人隐私。[19]上世纪八十年代英国颁布了《数据保护法》对个人信息安全问题提供了法律保障。[20]郭世斌等提到国外个人信息保护的立法模式主要有以欧盟为代表的统一法典模式和以美国为代表的分散立法模式。[21]德国学者克里斯托弗·库恩 2008 年《European Data Protection Law》一书中，主要对欧洲主要国家的法律文件进行了介绍、具体分析了有关数据保护的法律基本概念、国际间数据传输过程中的数据保护问题以及

对于公司应该做些什么来保护数据安全提供了非常详细的建议和指导，这本书对了解学习欧洲个人信息保护法律制度提供了一个很好的帮助。[22]

三是行业自律。美国学者 P．P．Swire 在其早前的一篇文章中，它提出在个人信息保护过程中不仅要尊重市场经济的规律，而且还应发挥政府作用，政府作为公共权力机关具有一定的强制力，但更重要的是，要激发出信息行业的自律意识，在个人信息管理上发挥“自我监管”的潜能。在他看来，纯粹的市场机制或纯粹的政府监管之所以失败，最重要的原因是他们忽视了信息产业的自律与政府管理的结合作用。因此，强调要重视发挥行业自律作用，制定行业行为规范，提高行业的声誉和技术水平。同时，在政府规范行业的帮助下，督促信息行业做出相应的调整，进而避免违反法律的禁令，以此来确保个人信息的安全。[23]尼格罗庞蒂提出提出利用经济手段（如税收减免等）激励网络服务运营商采取自我监管措施，从而达到减少网络安全问题的目的，从经济学的角度为提高网络监管的主动性提供了新的视角。[24]

四是限制政府权力的角度。林德尔.G.霍尔库姆提出了要怎样做才能达到在限制政府权力的同时最大程度上保护公民权利的问题，也就是说，如何协调互联网监管和互联网空间自由，同时实现保护网络用户隐私与网络监管的问题。[25]为了避免滥用政府网络安全监管权力，国外学者安东尼•唐斯提出了权力相互制约思路，用权力来制约权力，即部门之间相互制约、相互牵制，政府权力的扩大受到公共利益的制约，这是一种建立在大多数人共识基础上的规则。[26]

（4）个人信息安全事件频发的原因研究

Kruger.H.A 和 Kearney.W.D 提到网络用户个人信息保护意识淡薄是网络信息安全事件频发的主要原因，但现实中影响用户信息安全意识薄弱的因素太多，如片面追求眼前的经济利益、组织规章制度不严、缺乏信息安全保护知识等。[27]Colin Tankard 认为在大数据时代企业作为个人消费者个人信息收集者，而这些信息之所以很容易成为黑客攻击的目标，正是因为黑客也利用了这一点，因此越来越多的骚扰电话及短信如约而至的发送到了消费者的手机上。[28]丹尼尔·沙勒夫在其著作《隐私不保的年代》一书中指出，博客和社交网站中储存了大量与人们私人生活有关的个人信息，一旦这些个人信息因某一事件在网络群体中引起非理性的“人肉搜索”，就会发展成对个体的网络暴力攻击甚至会造成更严重的后果。[29]

1.2.2 国内研究现状

党的十八大以来，以习近平同志为核心的党中央以国家安全观为指导，对加强国家网络安全作出了重要部署。特别是自 2017 年 6 月 1 日起开始施行的《中华人民共和国网络安全法》这标志着我国网络信息安全管理进入了一个新的阶

段，这是我国网络信息安全管理立法进程中的一个里程碑。这不仅是中国共产党第一部网络空间治理法律，也是中国维护网络安全的基本法律制度，是网络信息安全管理上具有里程碑意义的重大法律事件。这些进步都可以看出，网络信息安全管理已上升到国家战略的高度。目前，我国学者对移动互联网个人信息泄露问题的研究，从研究角度来看，大致可分为：

（1）关于个人信息、网络个人信息的概念研究

我国学者周汉华将个人信息定义为“能够单独或与其他信息相比较来识别特定个人的信息，如个人的姓名、地址、出生日期、身份证号码、病历、人事档案、照片等”。[30]朗庆斌、孙毅、杨莉认为对于个人信息和个人数据而言，个人信息是既包括具有个体属性的个人数据也包括被处理过的个人数据，个人数据是个人信息的载体。[31]齐爱民认为“个人信息是指能够直接或间接识别个人身份的信息，包括个人的姓名、性别、年龄、血型、健康状况、身高、人种、地址、头衔、职业、学位、生日、特征等等”。[32]然而，进入信息时代后，网络隐私这一新的概念被提出，它在内涵上与传统的隐私概念基本一致，但在范围和内容上有所不同。胡皓渊认为网络隐私权是传统隐私权在网络空间的延伸，表现为个人信息的收集、使用和利用。在网络空间中，个人隐私以数字化形式表现出来，现代网络隐私权的概念主要属于个人信息资料隐私权的范畴，个人信息资料受保护不仅包括自然人在日常生活中信息（例如在日常生活中的行为习惯、生活方式和基本信息）不被人通过互联网这一媒介暴露的权利，也包括自然人在使用互联网过程中各网络行为所产生的网络个人信息不被非法使用的权利。因此，在这种环境下，个人信息除了作为自然人所附的个人资料外，还包括由网络活动所产生的更为重要的网络个人信息。[33]由工业部和信息化部联合其他部门在 2013 年 2 月出台的我国首个个人信息保护的国家标准《信息安全技术公共及商用服务信息系统个人信息保护指南》中将个人信息定义为“可为信息系统所处理、与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的计算机数据”。[34]我国《关于加强网络信息保护的决定》第一条规定：“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”。该条规定将个人信息分为两类，一类是能够识别公民个人身份的电子信息，另一类是涉及个人隐私的电子信息。换言之，个人信息包括隐私信息与非隐私信息。有研究进一步将个人信息与个人隐私信息的关系推导为，个人信息是个人隐私信息的上位概念，个人隐私信息是个人信息的一部分。[35]

（2）关于个人信息保护的法律层面研究

国内不少学者认为导致个人信息安全问题频发的原因很大程度上是因为缺少专门的关于个人信息安全保护的法令法规以及对个人信息权的界定不清楚。王

洋提出，我国政府在网络监管法律法规方面还未形成一个完整体系，从 2000 年到 2016 年，全国人民代表大会常务委员会仅颁布了四部与网络监管相关的法律法规，大量的行政法规甚至更低层次的部门规章在实际的监管工作中发挥着作用，而关于个人隐私保护和数据安全的法律尤其缺乏。[36]刘雪、胡敏洁分析了大数据背景下的网络隐私信息，提出要在两个方面不断努力，既要加强网络监管，完善法律保护，以此来营造纯粹的网络氛围。[37]李欲晓认为，在当今时代，加强个人隐私保护是重中之重，个人信息的保护应该上升到国家战略资源的高度，在法律层面给个人信息予以保护，要加快立法保障，政府部门要在以法律为依据的基础上加大监管力度。[38]刘德良教授认为，大数据时代给个人信息安全带来了新的挑战。在加强网络安全保护的同时，加快个人信息保护法的订立也是大势所趋。[39]张平教授提出，与我国的港澳台地区以及其他国家相比，我国还没有一部专门的个人信息保护法以及专门的个人信息保护机构，当个人信息受到严重侵害时，刑法和民法都不足以及时对侵权人进行处罚，也不足以对被侵权人进行有效的民事救济，因此，有必要制定专门的个人信息保护法来规范对个人信息的侵权行为。[40]陈红也认为，国家应制定专门的个人信息保护法，规范个人信息的收集、处理和使用行为，以使隐私权在我国专门法律中得到认可。[41]

（3）网络个人信息泄露的表现形式研究

王丽萍提到了侵犯网络隐私权的两种主要表现:一是对个人信息的不当收集；二是对个人信息的不当使用。[42]李德成列举了具体的方式:cookie 文件滥用；监控软件、识别机制的滥用；木马病毒；第三方泄露或共享。[43]秦尘阐述了在 web1.0[①]时期，网络用户主要通过搜索引擎获取信息，此时主要是黑客通过病毒、木马等暴力手段破解存储在硬盘上的信息泄露用户的隐私。在 web2.0[②]时期，随着网络视频的快速发展，网民，尤其是著名明星和爆炸性事件的主角的信息通过人肉搜索被泄露，在当今大互联网时代，社交软件应用和社交网络服务(SNS)已经成为一种趋势，互联网服务供应商有意或无意地通过漏洞泄露用户个人信息。[44]

（4）关于网络个人信息保护行业自律的研究

熊进光首先提出互联网时代的到来将对隐私权的安全构成威胁，并建议政府应该拓展监管手段来保护用户的隐私权。[45]张继红教授在 2018 年提出，个人信息保护中的自律管理是对政府监管中强制性方法的有益补充，可以有效发挥各行

[①] Web1.0 是以编辑为特征，网站提供给用户的内容是网站编辑进行编辑处理后提供的，用户阅读网站提供的内容。这个过程是网站到用户的单向行为，web1.0 时代的代表站点为新浪，搜狐，网易三大门户。

[②] Web2.0 更注重用户的交互作用，用户既是网站内容的消费者（浏览者），也是网站内容的制造者。（微博、天涯社区、自媒体）是以加强了网站与用户之间的互动，网站内容基于用户提供，网站的诸多功能也由用户参与建设，实现了网站与用户双向的交流与参与；用户在 web2.0 网站系统内拥有自己的数据。并完全基于 WEB，所有功能都能通过浏览器完成。

业自我监督、自我管理的优势。随着互联网和大数据的快速发展，强调在适当的政府监管下进行自律管理已成为新形势下个人信息保护系统发展的一大趋势。[46]卢小宾等进一步指出，为了在信息环境的大潮中真正保护公民的个人信息，仅仅依靠政府和个人是远远不够的，必学号召互联网行业的经营者也加入进来，即学习美国式的行业自律模式，加强行业自律，建立行业惯例，并给予技术支持，这样才能从这三个层面真正实现对公民个人信息的全方位保护。[47]在此基础上，田耀强调了行业自律的重要性，认为政府监管只能从外部限制公民信息的非法使用要真正实现合理合法地使用公民的个人信息，只有从行业经营者内部着手，行业内部严格要求并自觉遵守行业规则，实现从信息使用者到信息保护者的转变，形成最高级别的信息安全自我保护机制。[48]

（5）关于网络个人信息保护问题的研究

针对我国公民个人信息安全管理的现状，蔡文通认为公民个人信息安全监管是最突出的社会问题，如监管主体不清、多头监管、责任推诿、监管方式单一等问题导致监管低效，个人信息泄露频频发生等。[49]王慧军认为我国网络管理存在的问题包括：由于立法滞后，导致对网络违法犯罪行为的认定缺乏具体规范、由于政府管理职责不明确，管理效果不理想、由于网络技术落后，因此难以及时准确地发现网络违法行为等。[50]舒筠云提出在立法保护个人信息时应重点强化民事确权和民事归责，特别是当前的普遍情况是，信息侵权行为能够真正受到惩罚的往往只是冰山一角，只有当个人信息泄露达到一定数量、涉及面广或造成严重后果时，刑法才会介入。对单个信息主体的信息被侵犯或者信息泄露情节不严重的，很难处罚。这会促使信息处理者为了获得更大的经济利益，研究法律的漏洞，肆无忌惮的打起擦边球，游走在非法使用公民个人信息的法律边缘。[51]肖成俊、许玉镇提出我国政府监管过程中缺乏专门的个人信息监管机构，在利用大数据技术挖掘个人信息价值的过程中，他们更多地依赖于政府部门或其他信息处理者的自我意识，这都是因为行政监督力度薄弱。没有独立的行政监督机构的监督，很难对政府部门或其他信息处理机构进行监管，因此，公民个人信息的安全无法真正得到保障。比方说在《电信和互联网用户个人信息保护规定》的相关法律条文中，指出电信管理单位必须对公众信息保护行为进行监督（此处提及的电信管理单位主要是指工信部和各省市通信管理部门），但是，对于监管流程的具体实施办法却没有相应的规定，使得电信管理单位在实际操作过程中对该规定的实施和执行还没有得到充分的落实。[52]

1.2.3 文献评述

随着信息安全问题上升到国家安全的层面，强化信息安全防御、研究制定信息安全管理策略已被各国政府纷纷提升到国家战略高度，特别是近几年移动互联

网技术的飞速发展，使得信息安全管理变得尤为紧迫。

首先，随着移动互联网技术的高速发展，众多学者认识到信息技术革新在带来巨大价值及生活便利的同时也带来了个人信息保护方面的新难题，其中个人信息泄露问题便是其中的重点研究对象，因此互联网和大数据、网购、社交网络环境下的个人信息泄露与保护的研究内容逐渐增多。而在移动互联网个人信息保护领域的相关研究比较匮乏，相关的保护措施还处于探索阶段。

其次，通过对国内外研究现状的梳理可以发现，国内外学者都着重于从基础理论方面进行探讨且研究视角比较单一，比如个人信息等相关概念的界定、个人信息的立法保护、信息泄露原因等方面。

最后，从国内外学者的研究可以看出，国外更注重对具体领域的个人信息保护进行探讨，针对信息保护的专门立法完善，比如美国：在公民个人隐私权保护、未成年人保护、网络安全等方方面面都有专门的立法，取得了丰硕的成果。与国外先进的法律制度相比，我国的法律制度中还没有规范个人信息保护的正式法律。有关个人信息保护的法律法规分散于《宪法》、《中华人民共和国侵权责任法》（以下简称《侵权责任法》）、《中华人民共和国刑法》（以下简称《刑法》）以及全国人大常委会的相关决定、国务院及其部委的部门规章、地方性法规和行业自律公约等法律和规范中。

综上所述，本文以前人的理论成果为基础，详细阐述了个人信息概念、个人信息政府监管等基本概念，以此推动个人信息保护理论向更深层次发展，并且深入探讨移动互联网背景下个人信息泄露的特征与方式，从政府监管的分析视角出发，剖析移动互联网时代个人信息泄露政府监管现状及面临的问题，并对国外个人信息保护政府监管的特点进行比较分析，结合具体国情和时代背景，提出我国移动互联网个人信息泄露政府监管的路径构想，以便更好的在理论和实践两个层面上解决这个棘手问题。

1.3 研究思路与研究方法（Ways and Methods of the Study）

1.3.1 研究思路

本研究共分为六章，各章的主要内容分别叙述如下：

第一章为绪论，介绍研究背景和意义、国内外研究现状、研究思路与研究方法、主要创新点。

第二章为界定研究对象、阐述研究的理论基础及分析框架。首先对移动互联网、个人信息等概念进行界定；其次对理论依据进行阐释并建立移动互联网个人信息泄露政府监管的系统结构图，对该结构图进行分析，了解政府监管的相关要素，最后总结出基于监管系统的政府有效监管因素，为下文分析打下基础。

第三章为移动互联网个人信息泄露政府监管的现状与问题。具体分析移动互联网个人信息的监管主体的现状、监管依据的现状、监管手段的现状，并进一步分析当前政府监管中存在的问题。

第四章为系统结构视角下政府有效监管影响因素分析，具体分析各影响因素的不足，寻找政府监管不利的原因。

第五章为国外移动互联网个人信息保护的经验与启示，分析美国、欧盟、日本等国家现有的保护措施，为我国提供一定的借鉴。

第六章为完善移动互联网个人信息泄露政府监管的对策，根据前文中的现状、存在的问题及有效影响因素的分析，探讨如何优化政府个人信息保护的基本对策。

本研究的具体技术路线如图 1-7 所示：

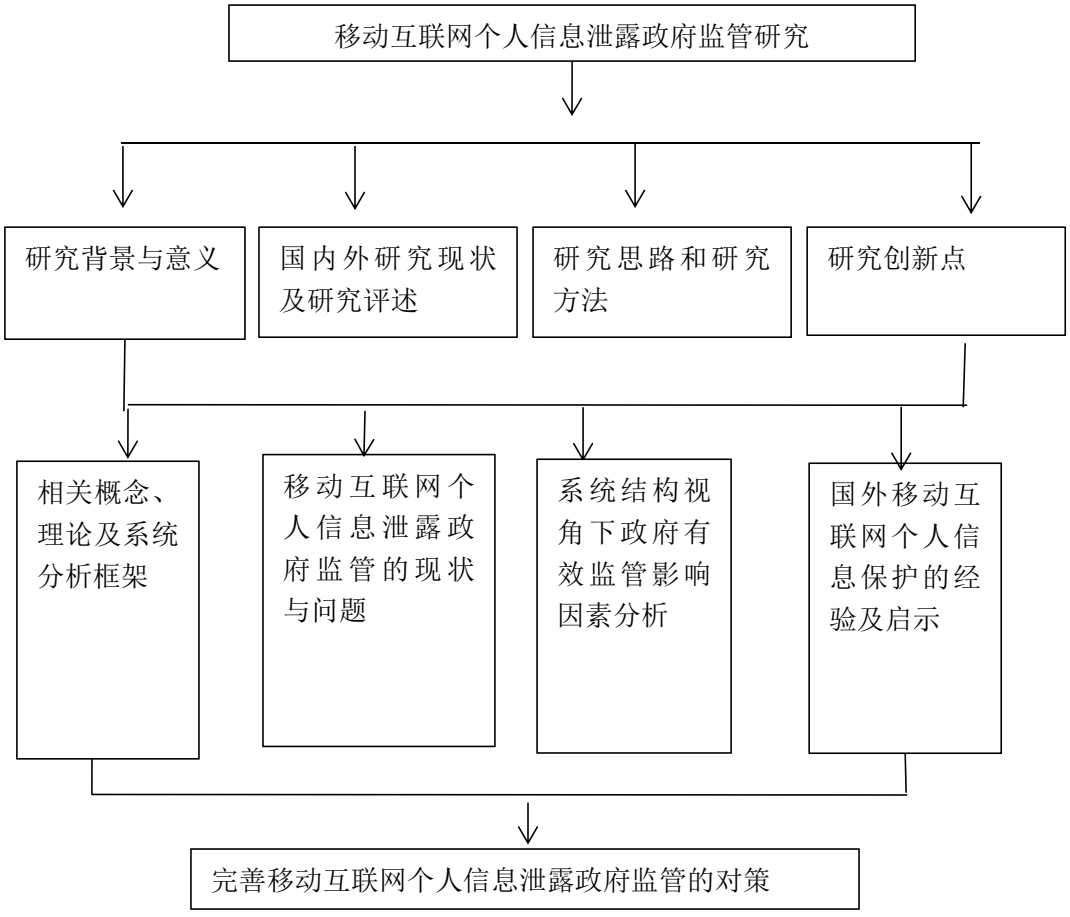

图 1-7 本文技术路线图

Figure 1-7 This paper technology roadmap

1.3.2 研究方法

文献分析法。文献是重要的学习参考资料，国内外学者对于个人信息保护的研究有着比较丰富的成果，通过检索相关的政策法规、调查数据、文献资料、研

究报告、著作、期刊论文、学位论文及国外文献资料等，并对相关资料进行整理分析，了解本领域的前沿成果和研究趋势，对前人的理论研究予以分析整合，为本文个人信息泄露政府监管路径的构想提供理论素材，并且本文一并收集分析了国外几个国家的监管经验，并进行了深入系统的研究，为我国个人信息泄露政府监管对策的构想提供了借鉴。

系统分析法。系统分析是一种系统的研究方法，它利用现代科学技术方法来分析与研究事物相关的系统的各种要素及其相互关系。本文将移动互联网个人信息泄露政府监管作为一个整体，对移动互联网个人信息泄露政府监管进行了系统分析，并详细分析了相关的影响因素。

比较分析法。比较研究是研究和判断事物与事物之间以及人与人之间的相似或相异程度的一种方法。比较研究法可以理解为一种按照一定的标准考察两个或两个以上相关事物的方法，寻找它们之间的异同，探索普遍规律和特殊规律。本文通过分析其他国家在移动互联网环境下个人信息泄露政府监管上的成功之处，发现其他国家在移动互联网环境下个人信息信息泄露政府政府监管方面的可供借鉴之处，为我国移动互联网环境下个人信息泄露政府监管对策提出建议。

1.4 研究创新点（Innovation of the Study）

1.4.1 研究创新点

本文主要创新之处首先在于研究视角上的创新，将个人信息保护置于移动互联网时代，将移动互联网与个人信息相结合，分析移动互联网监管中存在的比较重要的问题，即个人信息泄露的问题。从政府监管的视角研究个人信息保护问题改变了以往只从法学、信息通讯学或者整体角度进行研究的现状。个人信息泄露涉及到多个相关利益主体，在众多利益主体中政府居于主导地位，从政府的层面去分析个人信息保护面临的困境，并提出相应的监管路径，是保障个人信息权益的关键一环。其次，文章利用系统分析法，建立了移动互联网个人信息泄露政府监管系统结构图，基于该结构图进一步总结出了基于监管系统的政府有效监管因素，为更好的提出政府监管的优化对策打下基础。

2 相关概念、理论及系统分析框架

2 Related Concepts, Theories and Systems Analysis Framework

2.1 相关概念界定（Interpretations of Related Concepts）

2.1.1 移动互联网

（1）移动互联网概念

如今，我们日常生活的方方面面，无论是社交、购物、民生缴费等等一系列日常所需，伴随着互联网和移动通信技术的发展，基本都可以通过移动互联网这一媒介在任何时间地点实现线上操作。它可以说是一种现代商业生态环境，是在移动网络通道、商业理论以及移动网络技术的基础上发展起来的，其有着巨大的影响力，正逐步改变我们的行为习惯、生活方式等。那么究竟该如何来对移动互联网进行定义呢？2014 年工信部发布的《移动互联网白皮书》中就指出：移动互联网是指在提供互联网服务时与传统互联网时期大不相同，其在接入网络时是以移动网络为媒介的，包括 3 个要素：移动终端、应用服务、移动网络。[53]当前，移动终端种类繁多，例如笔记本电脑、平板电脑、智能手机等都可以归入移动终端的行列。移动网络从最初的 2G、3G 发展到当前普遍使用的 4G、wifi 以及开始在某些地区开始试点的 5G 等。移动互联网应用服务涉及范围很广，包括许多不同的应用与服务，如社交类、休闲娱乐类、工具媒体类、商业及移动支付类等。移动终端要想获取移动通信服务和互联网服务，在很大程度上依赖于移动网络。所使用的终端不同可以说是移动互联网与传统互联网使用过程中最大的区别，PC 端在传统互联网时期被广泛应用，当前日常生活中 PC 端的使用率有所降低，部分被移动终端所取代，因为移动互联网终端的移动性较 PC 端大大增强。人们可以借助移动互联网终端实时访问多样化的互联网“数据宇宙”，基本实现时时在线，无论什么时间、无论身处何地获取和处理信息的需求都得到了极大的满足。移动互联网极大地提高了国家、地区和城市在竞争与合作过程中的效率以及全球经济的发展速度和技术创新力。

（2）移动互联网的特征

移动互联网集移动通信的特性（如：随时、随地、随身）和互联网的特性（如：开放、共享、互动、创新）为一体，移动互联网许多其他特征的形成也与这些基本特征密切相关，可以把移动互联网的特征概括为以下几点：

1）用户身份信息不再是秘密

移动智能终端与 PC 端相比有很大不同，一般来说，当前的手机号码实名制

使得手机与用户绑定，手机与个人的身份紧密相关，换句话说，手机用户的身份不再是秘密，是可以被识别的，由此也使移动互联网具备了一些重要特点：

私密性更高。移动终端下由于用户身份信息已不再是秘密，而且其所留存的用户信息量远比 PC 电脑端高，相比之下移动终端的私密性较 PC 端大幅提升。

向用户推送的信息更具有针对性。由于移动互联网环境下用户身份不再是秘密，已能够被识别，而且经过对信息数据的分析，信息推送会更具指向性，因此用户也更容易被骚扰，例如，某些平台会根据我们的兴趣爱好推荐信息。

基于计费系统的运营模式。传统互联网时期的运营模式可以概括为广告模式，因为在这个阶段计费体系还没有建立，因此，很长一段时间互联网公司都一直依赖于广告模式，没有找到他们应该有的运营模式。但在移动互联网时代，因为身份识别已经实现，计费方式的业务管理模式不再是一个大问题。任何服务都是由计费系统支持的，业务模式不再是一个需要担心的问题，但与此同时病毒、木马等恶意程序也不断给人们带来困扰。

2）可被定位

移动终端不同于计算机终端，由于移动终端生产商将 GPS 等定位技术在移动终端系统开发时进行了应用，我们使用智能手机等移动终端时可以随时随地使用定位技术进行定位及导航，例如：当前微信 APP 的位置共享、百度地图等都是在此基础上开发的，给我们的日常生活带来了极大的便利。

3）相对封闭的网络体系

严格地说，用户可以自主决定网络开放与否，移动互联网是封闭性的，决定权在用户自身。

4）智能感应的终端体系

移动智能终端集计算、存储、通信等功能于一身，并具有了实用性很强的“扫一扫”、“附近的人”、“摇一摇”等智能感知能力。移动终端的智能传感功能，使移动终端在接入互联网的同时还催生了新的业务体系。

5）网络时时在线

传统互联网时期，受限于时间空间，电话、短信等功能我们可以随时使用，可以时时在线，大多数的互联网服务是不具备时时在线功能的。当前，移动终端在手，我们可以随时随地利用移动互联网获取我们所需的网络服务，不再受限于时间空间。

6）移动网络基本全覆盖

随着移动互联网技术的不断发展，移动网络、wifi 基本已经实现了全覆盖，而且上网速度也在不断加快，用户的使用感也不断提升。网络永远在线，信息实时接收，携带移动终端已经成为用户的日常生活习惯，但也导致信息像病毒一样

以极快的速度开始大范围传播。

2.1.2 移动互联网个人信息

（1）个人信息

我们应该首先在理解“信息”含义的基础上，去进一步解读“个人信息”。信息首先不是虚构的，必须是是真实客观存在的；信息可以间接证明物质的存在，以上是从哲学范畴对信息进行定义，反映了信息的哲学本质。[54]

实际上，在信息概念上，人们很难理解且还未形成统一的意见，但人们普遍认同信息具有客观性、可用性、共享性、依赖性、可分离性和可传递性等基本特征。

“个人信息”的概念可以说是由“信息”的概念延伸而来，诞生于信息社会。基于社会的现实情况进行分析，个人身份、家庭信息、生活背景、收入财产等与个人有关的一切资料都可以归属于个人信息的范畴。

工业和信息化部颁布的《电信和互联网用户个人信息保护规定》中将用户个人信息定义为：电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。[55]

进入网络时代后，个人信息的含义在网络环境下也出现了新的延伸，主要表现为用户个人信息的电子化。具体来说可分为两种情况：一是用户现实生活中的个人信息（如：身份证号码等）的电子化过程，任何在现实生活中属于个人信息范畴的信息，在我们使用智能手机等移动终端设备的过程中个人信息都会被有意或无意的收集，进而被转化成了网络环境中的个人信息；二是用户使用互联网的过程中产生的个人所特有的用户信息，例如 QQ 账号，邮箱、支付宝账号等。在当前网络环境的影响下，用户信息保护重心也应随之转移，应该把重点放到个人信息可能在网络环境中留存下来的各个环节上（例如：收集、处理环节）。

（2）移动互联网个人信息

根据上述对相关基本概念的梳理，文章对移动互联网环境下个人信息进行分类，大致归纳为以下四个方面：移动身份信息、移动网络行为信息、移动网络社交信息和移动终端信息。

1）移动身份信息

移动身份信息可以从两方面来说：一是现实中与个人相关的所有信息已基本实现电子化的转变（如我们姓名、性别、年龄等等一系列基本信息在我们使用移动互联网的过程中都留下了痕迹，形成了电子化的个人信息）；二是网上身份信息，单纯指我们在使用移动互联网的过程中生成的具有个体识别特征的信息（如

邮箱地址、微信账号密码、支付账号等）。

2）移动网络行为信息

我们在日常生活中使用移动终端系统的各种 APP（如：浏览器、支付宝等支付软件、阅读软件、音视频软件、淘宝等网购软件）的过程中产生的浏览记录、支付记录、休闲娱乐记录、交易记录等活动轨迹，以及这些 APP 平台利用这些活动轨迹进行分析处理而获取的有关用户个人阅读兴趣、消费偏好、个性等具有巨大商业价值的信息。

3）移动网络社交信息

主要是指我们在使用微信、QQ 等一系列即时通讯应用，微博等移动社交 app 的过程中，与他人分享及互动时所生成的一些信息。

4）移动网络终端信息

移动网络终端信息主要包括现在的云端信息，如百度云盘，手机品牌自带的云端等；定位获得的位置信息，一些软件在使用时要求获取位置权限；移动终端里的文件，如视频照片、便签记录、联系人等；手机通讯信息，如通话记录等；手机设备信息，如在微信朋友圈、微博等软件分享信息时会自动显示所使用的手机型号等。

（3）移动互联网个人信息泄露

指留存在移动互联网环境下的个人信息在未经个人授权或尚未得到依法有权公开个人信息的部门许可的情况下，却被非法披露、非法出售或者非法使用，信息主体对个人信息完全失控。[56]

（4）移动互联网个人信息泄露的特点和途径

1）特点

范围广：我们的个人信息由于网络平台的开放性、便捷性、共享性被更多的移动互联网运营平台收集，涉及的个人信息深入到生活的方方面面。因此，个人信息一旦被泄露，泄露范围之大往往难以估计。

易操作：随着信息技术的发展，各大网站、通信及软件运营商都有能力收集用户个人信息和互联网使用轨迹，一旦某一环节的运营商不履行用户个人信息保护职责，那么个人信息随时都可能面临被泄露的危机。

渠道多：个人信息可以通过硬件或软件泄露，也可以通过各 APP 平台泄露，也可以被黑客、木马病毒等非法窃取。

程度深：伴随着移动互联网通信技术的发展，个人信息泄露的程度较以前呈现出逐渐加深的趋势，从以前的个人位置和文件盗取发展到现在的浏览历史、账号密码等更为详细、具体的个人信息被泄露。

2）途径

各种 APP 应用软件：从表 2-1 可以看出各种不同用途的 APP 应用软件的下载并使用的用户规模及使用频率，即使是用途、种类大不相同的应用软件，却都有一个相同点，那就是在下载并使用时有极大的可能性会要求我们对其进行授权，一旦授权这些应用软件可能会在我们无意识的过程中收集很多个人信息，这些个人信息在被收集时以及收集后的分析使用过程中，如果用户个人信息保护不被重视或者保护措施不到位就很可能造成用户个人信息的泄露。

表 2-1 各类手机互联网应用的使用率

Table 2-1 Usage of various mobile internet applications

应用	用户规模（万）	网民使用率
微信等即时通信软件	69359	92.2%
浏览器等搜索软件	62398	82.9%
新闻资讯浏览软件	61959	82.3%
音乐播放器	51173	68.0%
视频播放软件	54857	72.9%
网上支付软件	52703	70.0%
淘宝等网购软件	50563	67.2%
百度地图等导航软件	46504	61.8%
各种网游软件	40710	54.1%

移动设备丢失：如果手机等移动设备不慎丢失，那么我们的个人信息很可能被其他人读取甚至被传播扩散，后果相当严重。

wifi：移动网络的全面普及以及移动 wifi 的基本全覆盖，其便利性不言而喻，大大方便了我们的日常生活，使用智能手机等移动端的每个人都有极大的可能性需要随时随地上网，例如在旅行、购物中心和吃饭的时候都会有上网需求，因此会在不加辨别的情况下主动连接各种各样的 wifi。但过度依赖 wifi 网络却不懂辨别 wifi 网络安全与否，这就有极大的可能性导致个人信息通过 wifi 网络泄露。与此同时，大量的 wifi 破解软件被研发出来，例如：wifi 万能钥匙等，这种破解软件的诞生，只要我们连接的 wifi 被破解，那么你的个人信息也会被同步泄露，那么造成的损失也就难以估计了。

移动支付（扫码支付）：据 2017 年底相关数据显示，与 2016 年底相比使用互联网支付功能的用户大约增长了 10%，使用率更是高达 70%。其中，使用移动互联网支付功能的用户规模大幅提高，与 2016 年底相比增加 5783 万，已经突破了 5.27 亿，年增长率为 12.3%，使用率达到 70%。当前移动支付功能的应用范围不断扩张，从最普遍的打车、送餐、购物等个人消费外，当前公交出行等也都实现了扫码支付，现在我们基本不用特意在身上准备现金，一部智能手机基本就能满足我们所有的消费需求。因此移动支付已成为时下最方便且流行的付款方式，但在移动支付程序的使用过程中，人们需要将相关的个人身份信息提供给移动支付软件公司，这种类型的公司所收集的个人信息不仅私密而且数据量庞大，一旦其出现保护个人信息不利的现象，这将会导致数以千计的用户信息泄露，很可能会造成个人财产损失。

面部识别解锁：当前人体面部特征识别技术越来越成熟，并被各移动终端生产商广泛运用。当前所被使用的面部解锁功能大都安全性较高，但也有一些制造商由于技术跟不上等原因，在模仿面部识别的功能时仅运用 2D+软件算法，这面部特征识别解锁功能的安全性极大的降低。这种 2D+软件算法的技术识别过程是未知的，但不可否认这种算法存在一些漏洞，因为有一些用户发现某些具备人脸识别解锁功能的手机甚至可以通过照片解锁，此时手机可以说是毫无安全可言，手机中储存的个人信息被泄露的风险在无形中增大许多。

2.1.3 个人信息政府监管

个人信息泄露政府监管是指以政府为主体部门对侵犯个人信息的违法行为进行管制。具体而言是指监督当前对个人信息的保护程度，如个人信息是处于安全的环境下被充分保护还是由于保护不力等原因被非法获取用于某些未知的途径。[57]对个人信息保护来说，政府监督的作用不容忽视，只要方式方法得当会发挥巨大的作用。当前个人信息泄露问题通过政府监管这一途径能够在某种程度上起到预防及减少发生率的作用，进而尽可能地避免个人信息被泄露，甚至在发生个人信息泄露问题后能够及时采取措施给予补救。

从我国具体国情和时代特点的角度出发，笔者认为，从本质上讲，个人信息泄露政府监管就是指依据国家相关规定拥有行政监管权力的相关政府职能部门，以此领域的的法律法规为监管依据对真实存在且具备单一识别特征的个人信息进行保护，并且对侵犯个人信息的违法犯罪行为进行管制的过程。具体可以从以下三个方面来解释:第一，政府监管的对象包括对移动互联网运营商等在内的移动互联网行业在个人信息收集、分析等过程中发生的泄露个人信息的不法行为进行监管以及如何对其进行监管以减少该现象的发生；第二，个人信息保护是以相关法律法规为依据，相关监管部门对侵害个人信息安全的违法行为行使监管权，以国家的强制性为基础来实现监管目的；第三，由于当前的监管环境比较复杂，必须要确保监管机构在监管过程中能独立行使监管权，不会被其他个人和机构影响，处于完全独立地位，并利用合理合法的监管手段对侵犯个人信息的违法行为进行管制，把保障公民个人合法的信息权益不被侵犯作为工作的重中之重，维护社会秩序的和谐与稳定。

2.2 理论基础阐释（Interpretations of Theoretical Basis）

2.2.1 公共利益理论

施蒂格勒在 1971 年指出，公共利益理论以“公共意志”为出发点，代表了“所有人或者大部分的人”的最大利益，这是公共利益理论最主要的理念。在此之前，传统观点：政府监管是为了维护公众的利益，弥补市场调节机制的不完全

性缺陷，这一观点是被传统经济学家普遍接受的看法。换句话说，针对存在信息不对称、不完全竞争、公共物品、不确定性、自然垄断、外部性等市场失灵现象的行业，政府会采取相应的措施直接干预存在这些现象的行业主体的行为，从而达到在弥补市场失灵缺陷的同时又能维护社会公共利益的目标。这就是政府监管的“公共利益理论”。[58]从另一个角度来说，政府监管的公共利益理论其实是一种政策选择，主要就是为了应对市场失灵，维护公共利益。但是从当前对这一理论的研究来看，这一理论在某些方面仍然存在一些问题，首先对什么是公共利益，在界定方面难以达成共识，其次，监管者将公共利益置于优先地位的原因很难说明，最后克服市场失灵的最佳途径是不是政府监管也很难讲清楚。[59]

公共利益理论正是在市场失灵现象（垄断性、不完全竞争、外部性及信息不对称等）难以应对的基础上诞生的，为了应对这些问题，政府监管有其存在的合理性。如果自由市场不能有效地分配资源并满足消费者的需求，就需要政府来进行调控，且当监管范围能够恰好涵盖失灵范围时，此时社会福利也会随着政府监管而增加，尽可能的使多数人满意。通过分析研究发现，政府监管正是对市场失灵的一种反映，根据这一理论，政府可以制定科学合理的监管政策，并采取有效的措施来改善市场失灵现象，从而维护社会稳定。

以移动互联网个人信息保护中面临的信息不对称问题为例，导致个人信息被侵犯进而被泄露的一个非常重要的原因就是信息不对称。移动互联网运营主体在未经用授权及许可的前提下，一味的追逐商业利益，对用户的个人信息进行分析、加工处理等“二次利用”，其用数据分析的结果为用户提供个性化服务，迎合用户的兴趣爱好，进而实现自身经济利益的最大化。但与此同时，信息收集主体过度分析和利用用户个人信息的行为，恰好反映出其丝毫不顾及用户个人信息的安全，这不仅可能会使用户遭受精神上的打击更甚至会造成用户财产损失，给用户带来二次伤害，严重侵犯了个人信息的合法权益。用户对运营主体的上述行为却往往一无所知，不知道谁收集了自己的信息，又如何进行了使用，这些情况根本无从得知，可见信息不对称的现象相当严重。因此要寻求政府监管手段的帮助，缓解市场失灵现象，探索既能合法有效利用个人信息又能避免个人信息被泄露的有效路径，为个人信息的保护提供帮助。

目前，从我国现实情况来看，首先，中国的移动互联网行业起步晚于美国等国家，当前移动互联网运营商缺乏应有的的公共责任感。一般来说，要解决个人信息泄露问题，各移动互联网运营商参与进来是必不可少的。然而，由于移动互联网行业自律意识薄弱，这也是个人信息泄露问题不断出现的原因之一。其次，在自我保护意识及辨别能力方面，我国移动互联网用户在这方面的水平相对来说还比较低，依靠用户的自我保护、抵制和举报，起到的作用可以说是微乎其微的。

此外很多用户的维权观念比较淡薄，当他们发现个人信息遭遇泄露的时候，他们并没有意识到这可能会给自己的生活带来一些难以想象的恶劣的影响。政府需要逐步加大该领域的监管力度，使移动互联网个人信息市场的失灵现象得到改善甚至一步步解决，以此来实现保护用户信息权益的目的，为用户营造一个文明和谐的移动互联网世界。因此，基于公共利益理论，作为移动互联网个人信息泄露监管的重要主体，政府应该采取一系列措施对移动互联网各平台进行管理，以保护用户的合法信息权益。

2.3 系统分析框架(System Analysis Framework)

2.3.1 移动互联网个人信息泄露政府监管系统结构图

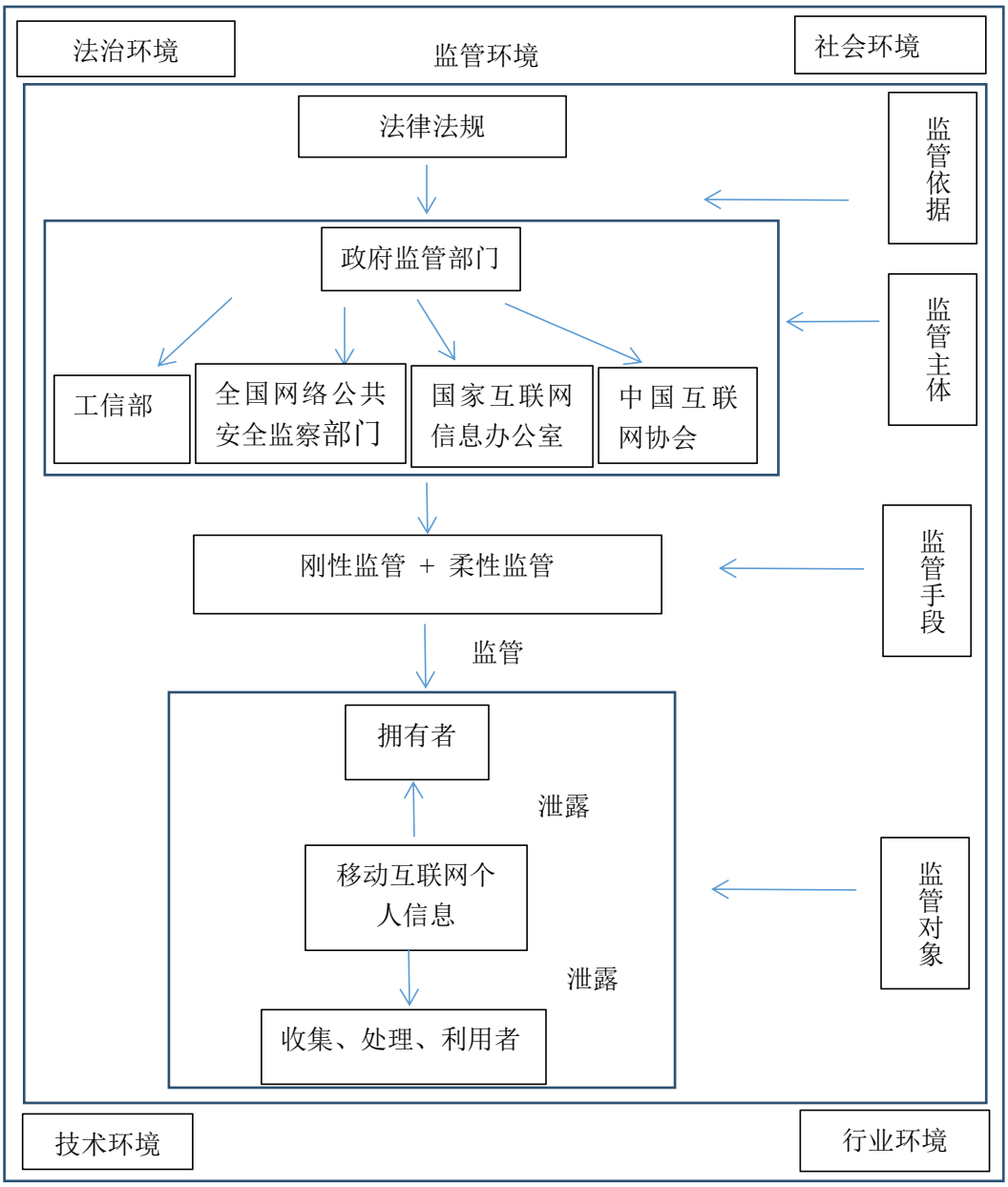

图 2-1 移动互联网个人信息泄露政府监管系统结构图

Figure 2-1 Structure of government regulatory system for disclosure of mobile internet personal information

移动互联网个人信息泄露政府监管系统结构图是指在移动互联网的空间内政府相关部门对由于个人信息的交换和传递而形成个人信息泄露问题进行监管。

在移动互联网个人信息传播链条中，信息拥有者、信息收集者、信息处理者、信息利用者等缺一不可，以上各方形成了一个完整的链条关系。在个人信息传递链中，每一层人员都必须按照一定的原则对信息进行管理和应用。只有这样才能保护个人信息不被泄露。任何环节的人员不按照相关的保密规则处理用户的个人信息，在每个环节都可能出现用户个人信息泄露的问题，使用户的个人信息面临严重的安全风险。

上图比较直观地显示了移动互联网个人信息政府监管系统结构图,下面详细解释移动互联网个人信息泄露政府监管结构图：

具有移动互联网监管职能的政府职能部门，依据人大立法、相关法规、部门规章等的规定，并运用刚性管理措施以及柔性管理措施相结合的手段，对使用移动互联网并留下个人信息的移动互联网使用者、移动互联网个人信息的收集者（使用者为了获取某些互联网服务，在移动互联网的使用过程中，授权各种运营商、平台、应用的运营者获取自己的个人信息，在这个过程中各种应用平台、移动设备等收集、保存大量的个人信息，这些平台、app 应用、网站的运营者都可以归为个人信息的收集者）、处理及利用者（收集个人信息的目的就是为了利用，因此各种移动互联网运营商即个人信息的收集者以及通过非法途径，如运用黑客攻击等手段获取个人信息并进行处理和利用的人，都是个人信息的处理利用者）的行为进行管制，预防发生个人信息泄露事件。[60]移动互联网上的个人信息其中涉及许多用户的私密信息，即使是一些常规信息它也承载着自然人的一般人格权，为了使用户的合法权益不受侵害，必须要运用恰当的手段来处理个人信息，确保没有丢失、损毁、泄露、篡改和不当使用等，以达到保护个人信息的目的。

明晰移动互联网个人信息泄露政府监管系统结构图具有重要的实际意义，可以指导政府的监管行为，政府在制定保护个人信息的对策时可以从相关各方来考虑。

2.3.2 移动互联网个人信息泄露政府监管系统构成要素

移动互联网用户个人信息泄露政府监管结构图的构成要素具体可分为：

（1）监管主体

监管主体主要是指具有移动互联网监管职能的相关政府部门，当前移动互联网时代，我国政府的网络监管模式与传统互联网时期相比并无太大差别，监管职权分散在多个部门中，实行多部门联合监管模式，各部门根据各自职责仅负责与

自己职责相关的一部分，当前我国的监管主体主要包括工信部、全国网络公共安全监察部门（即网监）、国家互联网信息办公室、中国互联网协会等。

（2）监管依据

我国一直推行依法治国，当前我国移动互联网监管依据主要分散在我国刑法、民法、消费者权益保护法及一些部门规章中，相关的法律法规还不完善，存在立法滞后等问题。

（3）监管手段

当前我国对移动互联网的监管手段在技术手段、行业自律手段、教育引导等方面都有所涉及，但由于我国互联网监管起步较晚，互联网更新换代的速度又很快，监管手段与互联网的发展速度来说还比较落后，相关的监管手段尚不完善，尚未形成完整的监管体系。

（4）监管对象

1）网络服务商。通常是指提供互联网服务或者运用互联网这一媒介提供服务的企业。网络服务提供商的种类繁多，以他们提供的服务为依据，大致可以把网络服务提供商划分为以下几类：访问服务、平台服务、内容浏览服务以及产品服务提供商等。访问服务提供商主要是指向用户提供网络接入服务，例如向用户出售移动网络数据的企业，当前最主要的网络接入服务提供商主要有以下几大家企业：中国移动、中国联通、中国电信，他们在很大程度上满足了人们接入互联网的需求；平台服务提供商主要是指各类满足人们各种需求的服务平台，例如社交网络、网络购物、电子商务等平台；内容提供商向我们提供各种新闻和咨询，例如微博、头条 APP 等；产品服务提供商为公众提供定制化的产品和服务，如乐视、优酷视频等软件公司。随着大数据技术的全面渗透，此类服务提供商有极大的可能性会成为侵犯个人信息的主要群体。

2）商业公司。个人信息的商业价值在大数据时代愈发凸显出来，其具有巨大的潜在价值，诱使许多商业公司为了追逐自身的经济利益，对个人信息过度利用，侵犯个人的信息权益。这些商业公司未经数据所有者同意，获取未经授权的数据，滥用和出售数据，也由此成为侵犯个人信息的另一个主体。

3）移动互联网用户。用户不仅是自身信息的创造者，同时也是各种信息的使用者，越来越多的人在日常生活中使用各种信息来满足他们个人甚至群体的需求。当前移动互联网用户规模不断增大，人与人之间的交流由于移动互联网的作用也变得越来越频繁，网络环境中留存了大量的个人信息，稍有不慎就有极大的可能会导致个人信息在这个过程中无意识的被泄露。此外，移动互联网用户还包含一个特殊的群体，即网络黑客，这个群体很容易通过技术手段窃取网络用户的个人信息。

2.3.3 移动互联网个人信息泄露政府监管的环境影响因素

移动互联网的个人信息环境是指与个人信息活动有关的所有自然和社会因素的总和，具有广泛而全面的特点。移动互联网个人信息泄露监管结构图的环境要素包括法治环境、社会环境、行业环境、技术环境等，具体情况如下：社会环境包括整个社会的政治、经济、法律、文化教育以及科技发展状况等；法治环境是指有关保护移动互联网上个人信息的相关法律的制定和实施；行业环境是指行业的自律组织、协会等及其所规定的行业自律准则等；一方面，技术环境包括移动互联网的位置位置和设备识别，网络安全防护，设备升级等。另一方面，监管人员的专业技术水平也可以归入技术环境的范畴。

（1）法治环境

法治，即依法而治，我国践行依法治国的基本方略，无论任何人在任何情况下都必须依法行事，尊重法律权威。移动互联网个人信息泄露政府监管的法治环境是必须从法律和制度上对移动互联网个人信息的实际掌握者加以有效制约与控制。法治环境的出发点与归宿点都是保护用户个人信息免遭非法侵害。政府监管法治环境的优劣，体现了维护用户个人信息安全制度化管理的程度和水平。政府需要尽快完善相关法律，尤其是要加快推进身份识别，隐私保护和个人信息保护等方面的法律建设。

（2）社会环境

社会环境也深深地影响着个人信息泄露问题政府监管工作的执行。政治因素，它包括用户发生个人信息泄露后维权机制是否建立、个人信息保护的法律法规建设情况等；经济因素指监管过程中财力、物力的投入使用情况、政府的财政支持力度等等；文化因素，它是指对个人信息保护的教育引导机制是否健全、信息安全宣传是否到位等。政府要加快推进社会信誉体系的建设、引导网民自发行为规范、自我安全意识增强。

（3）行业环境

政府相关制度建立的再完善，如果移动互联网所涉及的行业执行不到位，也难以发挥应有的效果。移动互联网企业自身加强对个人信息的重视度、保护度才能从根本上防止个人信息泄露问题。政府要加快建立移动互联网企业的行业自律机制，并督促相关企业的执行落实，充分利用移动互联网企业的行业自律制度，完善移动互联网个人信息泄露政府监管相关工作。

（4）技术环境

技术环境可以从两个方面来分析，一是指当前的移动互联网技术水平，例如当前 app 应用的位置定位技术及设备识别、安全防护、病毒查杀、设备升级等移动互联网领域技术手段的更新完善状况。二是政府监管人员的专业能力和职业素

养水平。个人信息泄露发生在移动互联网的大环境下，对政府监管工作提出了更高的要求，与现实世界中的监管工作相比大不相同，监管人员需要具备扎实的专业素养，掌握移动互联网领域的相关技术，更需要充分了解个人信息在移动互联网环境下的泄露途径和模式，要想胜任移动互联网环境下的个人信息泄露监管工作，必须要具备过硬的专业素养。政府要督促互联网企业不断更新升级个人信息防护技术，同时，他们必须重视提高自己的监管团队的专业素质水平。

2.3.4 基于监管系统的政府有效监管因素

在移动互联网个人信息泄露政府监管系统结构图及要素分析的基础上，基于监管系统要素，选取关键影响因素，进行总结分析，得出移动互联网个人信息泄露政府监管的有效监管因素，为下文进一步分析奠定基础：

表 2-2 基于监管系统的政府有效监管因素

Table 2-2 Effective government regulatory factors based on regulatory systems

L	R	I	T	E
legal	regulation	industrial	technological	educational
法律法规因素	监管机构因素	行业自律因素	技术因素	教育宣传因素

3 移动互联网个人信息泄露政府监管的现状与问题

3 The Current Situation and Problems of Government Regulation on Personal Information Disclosure on Mobile Internet

3.1 移动互联网个人信息泄露政府监管的现状（Current Situation of Government Regulation on Disclosure of Personal Information on Mobile Internet）

移动互联网技术的发展及其催生出的各种各样的 APP 应用，使我们的生活变得丰富多彩的同时，个人信息泄露问题在移动互联网环境下却也发生的更加频繁，形势愈发严峻，这也恰好暴露了我国移动互联网监管方面还存在一些问题，相关监管措施还不到位。根据相关法律法规和有关政策的规定，当前的监管形势是互联网领域的监管权分散在多个部门中，每个部门按照自己方式自行监管，与此同时，也开始利用行业协会等行业自律组织的作用，但就当前的情况来说作用不大；当前监管的主要着力点是对市场准入和市场行为的监管，例如，移动互联网运营商必须获得政府行政许可或或备案才能开始运营。下面对当前的监管现状进行详细分析。

3.1.1 监管主体现状

中国的互联网治理模式是多个部门都或多或少的拥有监管权，实行多部门联合管理。例如在网站设立、运营项目、内容审批等方面，各部门按职权自行开展审批工作。[61]有监管权的部门合力监管移动互联网的模式不仅反映了中国互联网监管的广泛范围和覆盖面之大，而且突显了中国互联网监管的困难和严峻性。但是，以上内容仍然是在传统互联网时期的监管模式。如今，移动互联网行业已成为时下主流，发展迅速，但监管机构尚未对此情况做出回应，并没有适应当下情况顺势而为。因此，一旦在政府监管部门应对能力不足的情况下发生个人信息泄露问题，情况严重甚至造成用户损失时，有关部门无法采取适当的措施及时阻止信息泄露，更何谈维护用户权益。

根据对相关资料的查阅并进行总结分析，下表 3-1 部分列举对网络信息安全具有监管职能的部门：

表 3-1 我国现有涉及互联网监管的部门

Table 3-1 Existing internet regulatory authorities in China

工业和信息化部	一般简称工信部，具有通信行业的部分管理权以及行业政策、标准的制定。在网络信息安全方面，其内部有许多机构都有所涉及，如:电信管理局、信息安全协调部等。[62]
全国网络公共安全监察部门	一般简称“网监”，当前大多数的公安部门都已经开始设立相关机构。所设立组织大都被称为网络监督机构或网络监督部门。其工作过程中也会受理与网络个人信息安全相关的问题。
国家互联网信息办公室	一般简称“网信办”，其工作重点放在互联网信息内容的管理上，并有权指导、督促各部门加大这方面的监管力度，并有权依据规定严查各类涉嫌违法的网站。
中国互联网协会	由其制定并颁布的《中国互联网协会章程》，其提出在保护行业利益的同时必须兼顾用户权益，更要重视加强行业自律。[63]

3.1.2 监管依据的现状

从现有的法律、法规来看，其中涉及移动互联网个人信息监管的内容可以划分为以下两个阶段：

第一阶段是在 2010 年之前制订的相关法律法规中，在保护个人通信自由、通信秘密及隐私方面，一些法律条文都有涉及，以上内容是此阶段我国的法律法规对个人信息保护的主要着力点。表 3-2 为该阶段相关的法律法规的列举：

表 3-2 我国 2010 年以前有关个人信息的保护的法律法规

Table 3-2 Laws and regulations on the protection of personal information before 2010 in China

序号	法律名称	颁布机关	颁布时间	相关内容
1	计算机信息网络国际联网安全保护管理办法	国务院	1997 年 12 月 17 日	对相关信息网络安全技术与管理人员加以限制，保护个人信息免遭非法攻击。
2	关于维护互联网安全的决定	人大及其常委会	2000 年 12 月 28 日	泄露公民通信机密将被追究刑事责任。
3	中华人民共和国刑法修正案（七）	人大及其常委会	2009 年 02 月 28 日	一些侵犯个人信息的行为，都会受到处罚，例如：通过不法途径获取信息，甚至将信息出售或者以其他方式提供给第三者。
4	中华人民共和国侵权责任法	人大及其常委会	2010 年 07 月 01	其中明确提到隐私权，并列入受法律保护的权利范围。

第二阶段是 2010 年之后制定的一些法律法规及部门规章等，这一阶段相关领域在立法方面较前一阶段取得了一些进展，以加强对个人信息的保护。表 3-3 为该阶段相关的法律法规的列举：

表 3-3 我国 2010 年以后有关个人信息的保护的法律法规

Table 3-3 Laws and regulations on the protection of personal information after 2010 in China

序号	法律名称	颁布机关	颁布时间	相关内容
1	关于加强网络团购经营活动管理的意见	国家工商行政管理总局	2012 年 3 月 12 日	团购网站上留存的消费者个人信息的保护力度要加大。
2	关于加强网络信息保护的决定	人大及其常委会	2012 年 12 月 28 日	规定了对网络上公民的个人电子信息提供保护，任何涉及侵犯个人信息的不法行为都会受到处罚，并规范了个人电子信息的保护范围，扩大了网络服务提供商的责任的范围，对相关主管机关及其法律规定的义务进行了说明。
3	信息安全技术公共及商用服务信息系统个人信息保护指南	工信部	2013 年 2 月 1 日	第一个个人信息保护国家标准。本标准最大的特点是，在未取得信息所有者明确授权之前，不得收集和使用涉及个人的敏感信息。
4	中华人民共和国消费者权益保护法	人大及其常委会	2014 年 3 月 15 日	其规定法律保护个人消费过程中被收集的个人信息，只有明确表明信息收集目的、使用目的、收集方法和收集范围等信息收集基本原则，运营商才能进行信息收集工作。
5	电信和互联网用户个人信息保护规定	工信部	2013 年 7 月 16 日	指出电信和互联网行业的用户个人信息同样受法律保护，并对电信和互联网信息服务供应商的职责进行了明确说明。
6	中华人民共和国网络安全法	人大及其常委会	2016 年 11 月 7 日	对网络信息安全作出了详细的规定。
7	中华人民共和国民法总则	人大及其常委会	2017 年 3 月 15 日	规定了个人信息的保护原则，规定法律保护与自然人有关的个人信息。

在上述列举的法律法规中，《网络安全法》可以说是迄今为止国内权威立法中在这一领域最全面的规定，并且相关条款更趋于网络虚拟世界中从立法角度保护个人信息的要求。因为，我国目前在个人信息保护上还没有专门立法，《网络安全法》提出的“合法、正当、必要”标准，初步提出了公民“知情同意”的个人信息保护模式，对用户的信息保密并保证用户信息安全，也对互联网运营商提出了保护用户个人信息的要求。首先，该法案首次明确定义了“个人信息”。其次，“用户信息”的概念也被提出，并且要求互联网服务提供商在收集用户个人信息或者其提供的服务具备收集信息功能时，提供商必须向用户明确指出并征求用户的同意。根据相关规定，“用户信息”的范围包括两个方面，可识别的个人

信息和与个人有关其他相关信息。再次，该法明确指出收集用户个人信息时要遵从够用原则并对所收集的信息进行匿名处理。在提供网络服务时严禁网络运营者收集不相关且不必要的个人信息，以减少过度收集和滥用给个人信息所带来的风险。在对待无法恢复且不具备特定识别特征的个人信息时，即一些匿名信息，在一定程度上允许运营商视相关情况决定提供与否而不需取得信息主体的同意，并可以通过此项规定，在一定程度上使个人信息保护与信息合法合理流动达到一定平衡。最后，该法对信息主体的删除权和更正权也作了明确规定，信息主体理应享有该权利。

此外，从以上两个表格的列举，我们不难看出相关法律规定涉及面较窄，并未完全覆盖个人信息保护的需求，而且大多较为陈旧，对如何保护个人信息还没有详细的立法规定。

3.1.3 监管方式的现状

目前，政府相关职能部门对移动互联网上个人信息泄露的主要监管方法和手段可以概括为以法律为重，政府引导、其他社会力量参与和许可备案等。在这一阶段，我国已经发布了有关网络信息安全的不同级别的法律文件。

目前，国家有关部门对网络信息传播的管理，基本上遵循以往对传统的媒体监督方式，实行分工协作，责任分担的监督模式。

移动互联网个人信息泄露政府监管的重点放在了对市场准入和市场行为的监管上，监管方式具体表现为各运营商要想进入移动互联网行业须首先获得政府的行政许可或进行相关备案。例如：许可和备案制在《互联网信息服务管理办法》第 4 条被明确指出。[64]同时，法律还规定，除了获得信息产业部门的营业执照外，每个经营者还必须获得相应营业领域主管营业部门的行政执照资格。可以说，双重许可备案和多部门联合监管是我国（移动）互联网行业的主要监管方法。

3.2 移动互联网个人信息泄露政府监管工作中的问题(Problems in Government Regulation on Disclosure of Personal Information on Mobile Internet)

3.2.1 监管工作中缺乏依据

首先，现有法律法规没有明确规定在整个移动互联网生态系统中，归属于系统上游的应用软件开发商、网络运营商、网络服务提供商等上游产业，以及设备与终端制造商和销售商等下游产业具体属于哪个部门的监管范围，特别是，它没有指定哪个部门或哪些部门负责监控供应商，以确保不会随意泄露用户信息。从现实情况来看，对移动互联网的监管监管模式较早期互联网监管时期并没有太大改变，由于所涉及的监管部门多，但是从当前的监管依据来看，在监管部门职责

划分上还没有明确规定，这就导致了相关部门无法及时采取有效措施去应对移动互联网行业中的个人信息泄露问题，这种情况下又何谈维护用户权益。习近平在十八届三中全会上指出了互联网多部门联合监管问题众多的现状，表明经过近二十年的快速发展，中国的互联网产业积累了很多问题，尤其是目前的监管体制不再适应快速发展的移动互联网产业。

其次，现行互联网监管相关的立法大多是部门规章和政策文件性质，但是部门规章和政策性文件并不具备较重的处罚权，由此导致在处罚泄漏用户个人信息违法违规行为时处罚往往较轻，法律也就起不到其本身该具备的惩戒震慑作用，那么也就无法有力打击个人信息泄露现象。例如，从经济学的角度来分析，对泄漏个人信息的惩罚相对较轻，违法犯罪的成本很低，打击力度低，难以真正起到威慑作用，这也间接导致了个人信息泄露监管工作效果不显著。

最后，在某些情况下，监管机构将面临无法可依，从而当出现泄露个人信息的非法行为时会发生处理不力甚至无法处理的的情况。关于移动互联网个人信息泄漏的政府监管政策和法规多是从宏观角度来提出的，侧重于原则性和指导性准则，但在微观层面上（如行业准入规则，信息保护原则，交易保护规则等）却缺乏具体可行的操作准则，真正监管时面临很大的困难。

3.2.2 监管部门职能冲突，监管效率低

众所周知，地震后 72 小时被称为黄金救援期。在此期间，受害者的生存率极高，此时救援效率的高低，将在很大程度上决定是否能更多的挽救受害者的生命。同样的道理也可用来分析个人信息泄露问题，在发生由个人信息泄露引起的不良网络事件（例如网络欺诈和网络暴力）之后，对于网监工作也同样存在追责的最佳时间。该时间段由于事件的传播范围较小以及给群众带来的影响较小，产生的社会影响还不算太坏，在此时网络监管者工作起来难度也相对较低。合理运用 IP 地址跟踪等技术手段，在第一时间锁定嫌疑人，能够对缓解眼前的危机起到很大的作用。一旦错过了这个黄金时间，网络监督机构在收集证据上就将面临许多方面的困难。随着移动互联网在电子商务，旅游，金融，自媒体，在线教育，在线医疗等行业不断拓展，所涉及的领域越来越多，这些行业经常会遇到泄露用户个人信息的情况。移动互联网的深入发展，在人们日常生活中的渗透率不断提高，也从侧面反映出移动互联网监管工作的环境变得更复杂，形势更加严峻。目前，尽管中国有许多移动互联网监管机构，但监管效率仍然很低。因为当严重的个人信息泄露事件发生时，监管部门首先考虑是“由谁管理”，而不是“如何管理”。监管职能的交叉重叠使得没有人愿意主动搅浑水，承担责任，严重影响了监管效率。

3.2.3 监管中责任追究难，维权难

现实生活中即使发生了泄露个人信息的违法行为，监管部门也很难取证。移动互联网归根结底仍然是网络空间，是虚拟出来，不同于现实世界，违法犯罪行为发生在移动互联网这一虚拟的世界中且由于其本身的特性（即时性、无纸化、电子化）使相关证据难以保存，网页信息、交易数据等证据不仅极易灭失也很难追查到犯罪嫌疑人，个人信息泄露问题一旦发生，政府监管部门执法和取证就会面临重重难关。具体反映在面临个人信息泄露违法行为，要想查找违法犯罪者非常困难，即使当前的某些手段可以用来锁定当事者，但当事者也有很多种途径来掩盖自己的不法行为。部分违法犯罪者非常狡猾采用拖、赖、躲的策略，甚至有部分犯罪者对如何躲避处罚非常熟悉，往往采取一系列手段，例如对网络电子数据进行修改、破坏、删除，甚至网站域名都更换。网络上的大多数电子数据均由掌握在运营主体及受运营主体委托的第三方手中，相关当事各方的配合对政府监管部门的调查取证工作至关重要。另外，基层监督部门在取证设备和手段上相对比较落后，增加了追责的难度，导致受害者要想真正维权也很困难。

3.2.4 监管人员技能不足，人数不足

一是现有监管人员对于应对网络监管工作的专业能力还有所欠缺。专业能力包括的范围极广，大底可归纳为两个主要的方面：网络技术水平以及相关领域法律知识的储备量上。在网络技术水平上，移动互联网个人信息泄露政府监管工作对监管人员在计算机技术应用水平上的要求十分苛刻，不仅必须对移动互联网使用相关知识融会贯通，更需要可以运用专业技能达到个人信息泄露政府监管工作的目的。比如说可以运用专业技能对网络上的各种信息进行数据分析，甚至是追踪侵犯个人信息等不良人员的 IP 地址、收集电子证据等来完成网络监管。其次，在职业素养方面，个人信息泄露问题发生在移动互联网这个大环境下，对监管人员提出了更高的要求。例如从监管人员自身法律素养的角度来看，移动互联网环境下发生的个人信息泄露问题，监管工作执行起来与现实生活中的案件大不相同，网络监管是应对虚拟世界的违法行为，而且当前与网络环境下个人信息泄露相关的法律制度还不健全，还存在一些漏洞，在这种情况下，对监管人员的法律知识储备以及法律敏感度有极高的要求。网络监管人员惟有能够遵守“四法”原则（知法、懂法、守法、用法），抓住侵犯个人信息不法行为的小尾巴，才有可能合理合法应对网络个人信息监管工作中各方面的要求，避免监管过程中“乱执法”问题。

二是执法人员数量不足。网络执法人员的部署远远低于网民增长速度。应对移动互联网环境下的个人信息泄露问题，政府监管人员需要具备较高的计算机信

息技术水平和过硬的职业素养。就目前来看，在专业素养和监管能力上，大多数监管人员或许并不欠缺，但从网络技术层次来讲，这却或多或少的成为了他们监管工作上的短板，进而难以满足变化多样的移动互联网个人信息泄露政府监管工作的要求。但与此恰恰相反的是，专业网络技术人员的监管能力和法律敏感度上又存在不足，并且我国行政部门对监管人员的选择十分谨慎，具备相应技术水平要求的人很难进人监管部门并胜任移动互联网个人信息泄露的监管工作。因此，当前监管机构的监管人员现状是专业监管团队规模较小，人手不足。

3.2.5 监管环境、对象复杂，监管困难

移动互联网应用人群不断拓展，对人们日常生活的渗透率不断提高，其承载的个人数据也呈井喷式增长趋势，但与之相应的是云计算、大数据等可以对个人信息进行数据挖掘、分析以及综合性处理的高新技术的亮相，使得个人信息保护工作成了新一代网络难题。以大数据技术为例，大数据技术可以对各型各色的个人数据进行综合分类、提取关键信息，最终获取针对性且实用性高的个人信息“结晶”。相关人员将这些成果投放在电子商务、政务等各个领域，无疑带来了可观的价值，潜在价值与明面上的价值都令人惊叹。可同时，个人信息被非法盗取、肆意使用及商用的可能性也大大提高，这带来的后果，即个人信息收集者等系列人员可能会对用户的消费记录、浏览记录等进行大数据分析，进而对每个用户进行精准分析，能够充分预测他们的行为、消费趋势、爱好等，即使是绝对性保密的付款密码和通信记录也将被轻松获取。恰恰相反的是，用户完全不知道是谁以及用什么方式收集、处理和使用了他们的信息，用户完全处于一种茫然的状态。可见移动互联网环境极为复杂，加大了监管的难度，不断出现的新状况和新形势也给政府个人信息监管带来新的挑战。

3.2.6 未充分利用行业自律监管

行业自律的辅助作用是不容忽视的，移动互联网行业也不例外。中国互联网协会、中国电子商务诚信联盟等是当前具有一定作用及认可度的主要互联网行业自律组织。当前互联网行业总体的行业自律现状是：缺乏明确的行业自律规则，依靠行业自律进行管制泄露个人信息的不法行为效率低下。现阶段看来，即使已经有部分行业自律公约，但大部分也仅仅只停留在文字和口头上，未发挥实际的作用，而且移动互联网领域的相关企业在商业利益的诱惑下，仅有的行业自律公约可能也无人遵守，变为“空头支票”。此外，从成立时间来看，国内各大知名网络公司成立时间不长，中小网络公司更是不计其数，每天还有大量新的网络公司建立，与此同时被淘汰的网络公司也数不胜数。抢占行业市场等想法的激化，也促使互联网企业在网络信息保护方面自我管控不严、越界行为不断发生。

4 系统结构视角下政府有效监管影响因素分析

4 Analysis of Influencing Factors of Effective Government Regulation from the Perspective of System Structure

本章节依据第二章对移动互联网个人信息泄露政府监管的系统分析，对在系统分析基础上形成的基于监管系统的政府有效监管因素进行详细的分析，即对政府监管的法律法规因素、监管机构因素、行业自律因素、技术因素、教育宣传因素进行详细分析，寻找移动互联网环境下发生个人信息泄露问题时，政府监管不利的原因，为下文提出有针对性的政府监管优化对策奠定基础。

4.1 相关法律法规滞后，法律体系不完善（The Relevant Laws and Regulations Lag Behind, the Legal System is not Perfect）

近年来，为了保护个人信息，中国颁布了一系列法律法规和规章等，以求能够为执行互联网领域个人信息保护监管工作的执行提供依据。目前，这些法律在一定程度上对移动互联网行业用户的个人信息保护起到了一定的积极作用。但是，中国与互联网相关的法律一般是在 2005 年前后颁布的，虽然在一定程度上对监管工作的执行以及保护个人信息避免不必要泄露发挥了效果，起到了一定的积极作用。但是这些法律法规的设立多是为了应对传统互联网时期存在的问题，尤其在个人信息保护方面涉及较少，相对落后于快速发展的移动互联网行业在个人信息保护方面的需求。因此，面对移动互联网领域突如其来的新问题和新情况，特别是用户个人信息的泄露问题，我国现行法律显得有点难以应对。

4.1.1 立法滞后，存在立法空白

在现阶段，适用于中国移动互联网的法律主要基于传统的互联网法律，还没有发布专门的“个人信息保护法”。由于立法滞后，旧的法律仍然被用来监督移动互联网的新领域，而现有的法律却不能在所有方面对其进行监管。结果，中国的移动互联网行业目前显示出“旧法律新问题”的监管局面。但是，快速发展的移动互联网行业催生了许多与用户的人身安全和财产安全直接相关的新兴问题，在面对这些新情况和新问题时监管人员却难以在现有法律中找到监管依据，相关领域法律上的空白和漏洞直接导致了监管工作中无法可依的困境。

首先，法律没有定义“个人信息”。法律没有明确定义什么是个人信息、其

范围和程度以及如何对其进行分类等。因为“个人信息”在现实生活中所涉及的范围及含义是非常广泛的，法律上却没有明确规定，因此要想对其进行分类和保护以及区分哪些与个人相关的信息受法律保护时就处于非常迷茫的状态。依此类推，例如，什么是“敏感信息”，什么是“重要信息”，涉及公共利益的个人信息如何公开，由于某些特殊情况被公开的个人信息是否还受法律保护，受法律保护的个人信息是否涵盖所有未被公开的个人信息，以及伪造的个人信息是否受法律保护等等。这些问题不能仅在理论层面进行讨论，还需要法律来回答和解决。

当前我国移动互联网用户规模不断增加，根据最新公布的数据已达 8.8 亿。同时，移动互联网具有覆盖范围更广、传输速度更快、影响更深远的特点，导致用户对自己在移动互联网上的信息逐渐失去控制力。当一件小事在移动互联网环境中成为公众关注的焦点时，假如是恶性事件就极有可能成为爆炸性新闻甚至是丑闻。由于移动互联网的用户群异常庞大，任何发生在移动互联网上的事件，如果涉及到的人较多或者被许多人关注，都可能成为公共事件，一旦事件被公布出来，影响范围之大难以想象。因此，当别有用心的人为了谋取非法利益或做出不当行为而使用移动互联网上的用户个人信息时，很可能造成不可预知的后果。

4.1.2 法律效力层次不高

由于我国现行法律缺乏涵盖网络信息保护各方面内容的综合性法律，因此不可能为网络上留存的个人信息提供全面而基础的法律保护。在现行法律中，保护个人信息的法律太少，国务院的行政法规和规章太多，还有一些地方法规，以及政府对某个领域或行业的一些指导方针或政策。

由于部门立法和地方法规通常仅适用于某个立法领域，因此它们的调整范围有限且适用范围有限，并且无法涵盖整个行业和领域的所有方面。同时，大多数现有法律层级过低且作用不大。结果，整个移动互联网行业的监管受到限制，对个人信息的法律保护显得鞭长莫及。

近年来，移动互联网的快速发展已经与传统互联网有了很大的不同。仅仅依靠有限的部门法律法规来解决移动互联网发展中出现的新问题、新情况是不现实的。随着移动互联网上涉及用户个人信息泄露的侵权案件的数量越来越多，冲突也越来越激烈，矛盾正在加剧。与移动互联网监管相关的法律法规和管理规定或多或少在各个部门的法律中都能看到影子。然而，缺乏统一性和协调性的弊端也非常明显，依靠部门的法律单独解决此问题是不现实的。因此，由全国人大及其常委会制定与个人信息保护相关的特别法已经变得非常迫切。

4.2 缺少统一、有效的监管体制（Lack of a Uniform and Effective Regulatory System）

目前，我国尚未建立统一有效的移动互联网个人信息保护监管体系。虽然与个人信息相关的一些相关部门承担监管责任，但这些部门专业性不足。专门的监管机构和有效的认证体系还没有建立，还没有形成成熟且可操作的监管体系，所以他们不能有效地帮助个人维护合法的信息权益。与此同时，在移动互联网环境下个人信息保护方面，某些相关部门都具有一定的监督管理权，但尚未明确划分各自的权限和责任。因此，在发生侵犯用户个人信息权益的情况时，各机构和部门可以独立行动，缺乏协调性，也可能出现相互推卸责任，无人监管的现象。因此，这种缺乏有效的事后权利保护机制和保护制度的情况下，使用户无法很好地维护自己的权益，这也会间接在某种程度上导致侵犯个人信息的不法行为更加猖狂。

4.2.1 缺乏个人信息保护专职机构

目前我国还没有一个专职机构来履行与个人信息保护相关的工作，依然延续多部门联合监管模式，导致相关部门在开展工作时存在职能交叉问题，未能实现各司其职，尚未有专门机构来执行个人信息监管工作，这不仅是我国政府在监管过程中存在的实际困境，也是政府在个人信息监管工作中的成效始终不好的原因之一。就像台湾地区、香港地区、新加坡都有专门的个人信息保护机构，他们的职能都存在一定的相通之处，都负责处理公众举报、组织调查相关情况、维护公众合法权益等等。专门的个人信息保护职能机构的缺失，现有与个人信息保护相关的部门为了履行保护个人信息的职责也制定和实施了一些政策，但这些政策在时效性以及效果上都存在一定问题。

以公安部、工业和信息技术部的专项行动为例，其在特定时期带头在全国范围内采取特殊手段打击侵害个人信息的行为。尽管特别行动在短期内的作用可以说是立竿见影，专项行动的严厉举措对违法违规者在短期内起到了威慑作用。此举只是一个临时措施，效果的持久性不长。这种临时性举措可能仅会在不当收集和使用个人信息现象态势非常严峻的情况下才会被使用，而且也很可能是迫于社会舆论的压力而无奈采取的举措，这种方法在短期内看效果极好，但从长远的视角看，这一举措要想长期发挥预防侵犯个人信息的不法行为的作用还是非常困难的。从本质上讲，它属于中国传统的治理结构（运动式治理）在当今时代的延续和发展，对形成保护个人信息的长期治理机制并起不到太大的作用。在短期内，政府有关部门采取的特殊行动确实符合公众的利益，既加强了对个人信息的保护，也减轻了舆论的压力。但是，这也恰好可以看出，专项行动并没有持续不断

的发挥作用。采取特殊行动的余热消失后，针对个人信息的违法犯罪行为也会再次猖獗。例如，在电信和互联网行业，工信部根据《电信和互联网用户个人信息保护条例》和其他文件的要求，率先带头开展打击个人信息犯罪行为的专项行动。经过专项特别行动之后，电信和互联网行业中的侵犯个人信息的乱象在短期内得到了有效的净化和规范。但专项行动过后，此前的乱象又开始慢慢蔓延开来，非法侵犯个人信息的的状况又开始大面积爆发，特别是在互联网领域，专项行动的余威越来越小，正如对信息安全状况的研究结果一样，根据中国互联网网络信息中心每年对用户进行的调查报告也显示，互联网已成为个人信泄露问题的重要发源地，然而，互联网行业缺乏专门的政府机构来对个人信息的收集和使用状况进行严格的监督，政府在保护个人信息方面的治理绩效也久久得不到提升。

4.2.2 监管体系中事后维权机制不完善，个人维权参与度低

监管部门尚未建立完善的移动互联网用户维权机制，此外当前的维权宣传还不到位。与传统线下维权事件相比，移动互联网个人信息泄露纠纷所面临的问题就复杂的多了，对执法人员素质和维权处理机制提出了更高的要求。目前，相关监管部门尚未携手建立用户维权信息共享和执法互动平台，许多用户对当前的网络侵害维权方式并不熟悉甚至一无所知，最终导致放弃维权。用户不知如何维权，维权参与度低，这是移动互联网时代个人信息泄露维权工作所要面临的巨大挑战。

在现实生活中，我们得知，当前很多用户经常收到垃圾短信、诈骗电话、推销信息或一些不相干的垃圾邮件等，他们已经意识到自己信息在某种程度上被泄露了，但由于这在日常生活中是司空见惯的情况，只要未受到严重的损失，我们往往会选择忽视，对这种现象保持沉默。更重要的是，由于存在信息不对称，即使在使用移动互联网后，个人信息在被过度收集和利用后被泄露，用户往往无从得知到底是谁最先收集了自己的信息，以及后来经有谁手被转卖，这些情况用户根本无从得知，要想找到信息泄露的源头以及途径根本就是天方夜谭。即使当前已经具有了一些防范手段，但想要应对当前个人信息泄露的现状也是困难重重，监管机关的调查和取证工作亦无从下手。除此之外，在法律专业知识和经济实力方面，运营商拥有的资本要远远强于移动互联网用户，运营商有经济实力赔偿用户因非法获取或使用用户个人信息而给用户带来的经济上的、精神上的损失。恰恰相反的是，要想在开放、共享的虚拟网络世界中取证是异常困难的，许多用户也知道这一情况，当用户的个人信息权受到侵犯时，用户面临的将是漫长的举证过程、高昂的诉讼费用、以及其他不确定性因素等，更深层次的原因是大多数用户根本不知道该找哪个机构维权，再向公安局等机构申诉时往往会被以各种原因拒之门外。在损失较小或没有损失的情况下，用户往往会选择自愿放弃依法捍卫

自己的权利，选择沉默。众多现实案例表明，侵害个人信息的行为之所以有增无减，政府维权机制缺失是一大原因，与用户信息安全意识淡薄也有着莫大的联系。个人信息安全保护意识淡薄的表现具体可见下图 4-1：[65]

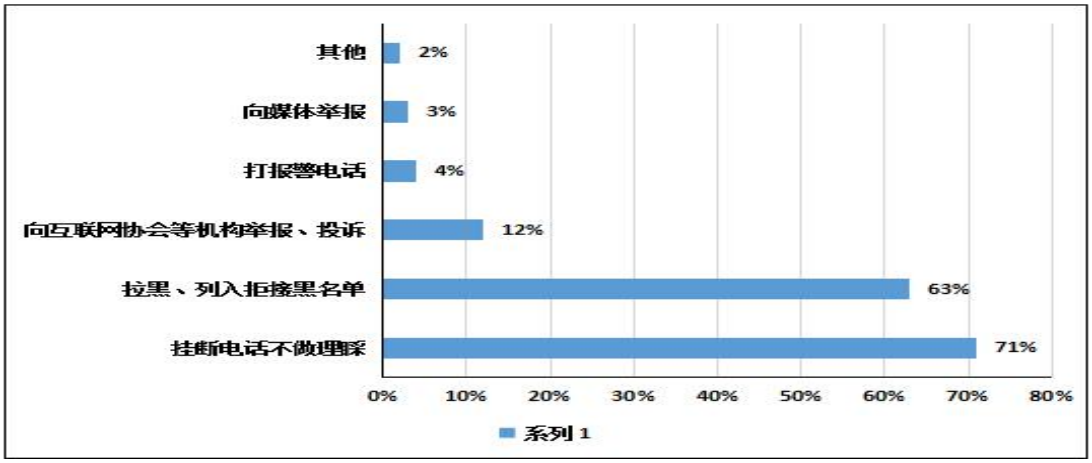

图 4-1 个人信息保护意识淡薄的表现形式

Figure 4-1 The expression of weak awareness of personal information protection

4.3 政府未建立完善的行业自律机制(The Government has not Established Perfect Industry Self-discipline Mechanism)

4.3.1 缺少行业监管主体

移动网络应用程序的形式众多且复杂，要想应对移动互联网环境下的个人信息泄露问题，政府要引导行业自身发挥出应对个人信息泄露问题的辅助作用，那么首先要做的就是界定行业监管主体。然而，我国目前还没有依法对行业监管机构进行法律界定，当然也没有形成有效的行业监管体系。中国互联网协会有权对互联网上存在的一些不法信息进行监管，但其作为当前主要的行业自律组织之一，实际上互联网协会的权利非常有限，只能发挥很小的作用，大部分的监管权依然集中在政府行政部门。在中国的行业监管法律中，在大数据监管部分目前更多的是制定了具体的指导性政策，从实际操作性的角度来说就比较弱，此外，政府监管的范围并没有实现整个移动互联网领域的全覆盖，也就很难发挥其监管功能以补充行业自我规范的不足。在缺乏监管的情况下，移动互联网用户的个人信息容易受到侵犯处于较脆弱的状态，必将影响互联网产业的健康发展。

4.3.2 缺乏具体行业监管规则

在移动互联网产业发展的早期阶段，人们追求的是发展速度，一直在追赶发展的步伐。然而，目前我国还没有形成统一的行业自律规则，政府部门已经在着手建立行业自律规则，但仍处于早期阶段还不成熟，这也导致了网络行业监管细则的缺失，这一观点已经获得了人们的认可。关于个人信息和网络数据的使用，中国尚未制定保护它的特殊法律，在移动互联网企业运营过程中，在收集信息、

数据使用方面也没有受到行业内部的自我约束，这是企业侵权事件时有发生重要原因之一。通常根据行业发展的问题和特点来制定具有针对性的行业内部监管规则，它们非常实用且具有很强的指导性，而缺乏行业内部的个人信息保护细则，导致行业发展的无序。

4.4 政府教育宣传引导不足(Lack of Government Education and Publicity)

4.4.1 专业人才供给严重不足

网络安全人才在全球范围内仍然是稀缺资源。虽然政府已经通过在高校设立相关专业等办法来逐步解决此问题，高校网络安全人才培养速度远远落后于快速发展的网络安全市场，市场缺口超过 90%。根据相关分析，到 2020 年，中国对网络安全人才的需求将达到 160 万，而每年只有 1 万名网络安全专业毕业生。这也导致了当发生移动互联网个人信息泄露问题时，政府监管工作始终比较吃力，成效不显著的原因之一。

4.4.2 个人信息保护教育宣传力度不足

政府未充分开展宣传工作，移动互联网用户网络行为较为随意，随意向网络运营商提供个人信息，对保护自身信息这件事还未引起足够重视。目前，许多移动互联网领域的运营商不遵守信息收集规则，存在超范围收集个人信息的现象，而且此类现象比较普遍。例如当我们初次使用的某些应用程序时，就会弹出一些窗口，意图定位我们的位置信息,以及获得阅读我们的短信,联系人等权限,在许多情况下,这些都是不必要的,即使不提供这些信息也完全不影响我们使用这些软件，当然也存在部分软件如果我们不对其进行收集信息的的授权，那么我们可能无法应用该软件或者其部分功能不对我们开发，这些行为其实都是不可取的。但站在用户的角度而言，用户相对处于弱势，为了使用软件，不管是迫于无奈还是自愿都会向软件开放授权，完全不具备信息保护意识和能力,往往完全按照运营商的要求填写,并不会去辨别某些授权是否是必要的，甚至对平台出示的个人信息保护声明，不进行浏览及阅读，直接勾选同意平台的相关要求。虽然大多数平台出具声明的意图并不是为了更好地保护个人信息,也只是为了逃避自己的责任。用户自身随意泄露自己的信息，不注重信息保护，保护意识不足，可以说是个人信息泄露的源头。

个人信息保护的第一道防线原本就应从用户个人角度进行考量，政府在监管过程中却未对其进行充分利用。但要想真正保护个人信息离不开用户自身的信息安全素养和保护技能，因此，只有通过不断提高自己的知识和能力来保护个人信息安全，建立自我保护的“防火墙”，在面对个人信息安全的威胁和挑战时，才

不至于手忙脚乱。虽然当前在中小学道德和法制教育中互联网法律法规和网络伦理道德教育已经有所涉及，但尚未被正式纳入现行的国家教育系统，很难真正普遍提高用户自身的信息安全素养和技能。

4.5 监管技术落后，政府支持力度不足（ Poor Regulatory Technology and Inadequate Government Support ）

4.5.1 网络安全技术落后

网络安全技术的先进与否，是否能跟上互联网的发展步伐，是保护个人信息的基本要求。但我国网络安全技术水平的现实情况是，由于起步晚，不论是网络硬件还是操作系统相对来说远不及互联网的发展速度，比较落后。调查显示，我国大约 67%的信息产品和技术是从国外进口的。那么硬件设施或操作系统性能的安全就很难保障，很可能存在陷阱。[66]此外，许多发达国家的一些方针政策不太利于中国的网络发展。中国信息安全专家徐民斌表示“在大数据分析技术和平台上过度依赖于国外，存在信息泄露的隐患，其他国家可以通过大数据分析平台获取敏感的数据情报，分析中国经济社会发展的脉搏，从而威胁到中国的国家安全”。[67]胡利泉也提出了“谁掌握了信息、就掌握了未来”的观点。[68]2013 年美国棱镜事件被曝光，我们有充分的理由可以怀疑，美国一直掌握着包括中国在内的许多其他国家的机密。我国在网络技术方面掌控力、自主性不足，落后于网络起步早的国家，使得网络信息“生命线”被交到了其他人手中，又何谈保护网络环境下用户的个人信息。与把网络技术运用得心应手的违法人员相比，中国监管部门的监管人员在网络信息安全监管技术的运用上还存在许多不完善的地方，甚至还有不少部门还在沿用传统的人力侦查的监管模式。公开资料显示，直到 2016 年，人民法院才最终告别人工统计的时代。[69]技术力量跟不上，只会额外耗费更多的人、财、物，结果还发挥不出应有的效果，监管起来就如同大海捞针。此外在资金投入、技术人员水平、监管技术水平上还与监管部门的级别有关，级别越低，资金投入越少，信息技术人员配备不足，监管技术越落后。

4.5.2 移动互联网监管支持力度不足

财政支持力度对于培训网络监管人才，进行网络监管技术研发以及对设备进行更新都是必不可少的。但是，中国政府更倾向于在互联网和制造业一体化的关键领域增加金融投资，并没有动用足够的资金来支持互联网监管。

5 国外移动互联网个人信息保护的经验及启示

5 Foreign Mobile Internet Personal Information Protection Experience and Enlightenment

5.1 国外移动互联网个人信息保护的经验(Foreign Mobile Internet Personal Information Protection Experience)

在对其他国家的个人信息保护监管现状进行研究分析时，从现有的资料可以看出，多数学者把研究重点放在了美国和欧盟的现有的保护手段上。美国的行业自律模式可以说是比较完善的，其监管特点是以行业自律为主导，各方面的分散立法起辅助作用。而欧盟在立法方面则与美国正好相反，其在立法方面系统性较强，此外还建立了统一的监管机构。然而，中国本身是一个亚洲国家，如果只学习借鉴欧洲和美国的方式，难免会存在一定的偏差。因此，当在移动互联网环境下发生个人信息泄露问题时，为了更有针对性的提出优化政府监管的对策，要在尊重我国国情的前提下，学习国外个人信息保护机制的先进之处，文章以美国、欧盟、日本三个国家或地区为例，对其政府在个人信息保护上的经验及特点进行分析讨论。

5.1.1 美国移动互联网个人信息保护的经验

（1）分散立法

美国早在 1974 年就已经开始重视公众隐私权的保护，其颁布了《隐私权法》，这是美国第一部关于隐私权的立法，其中对使用用户的个人信息（个人记录）进行了规定。以名字为索引来向系统中进行数据输入操作，这是美国的惯例，并且个人记录就是使用该名称保存的所有信息。它既包含一些代表个人的基础信息（个人的照片，使用过的姓名，指纹，汽车牌照，驾照号码等）还包括一些特殊信息，（志愿者服务时间、医疗记录等），几乎涵盖了与个人有关的各种形形色色的信息。[70]该法规定要想使用个人信息必须取得当事人的授权才可以，其中也对公权力机关使用个人信息进行了规范，在对个人信息加以利用时即使是公权力机关也必须严格遵守隐私法中所批准的范围和权限。除了《隐私权法》这一专门性法律外，联邦法律中有将近 40 部都是与保护个人隐私相关的，表现出多样性和分散性的特点。在部门法、规制公权力行为法、以及在立法调整其他事项时都对个人隐私保护有所涉及，涵盖了科学、教育、文化、金融、保险等方方面面，范围非常广泛，对涉及个人隐私的许多细微方面都进行了立法保障。这些立法从方方面面对个人信息保护都做出了非常严格及详细的规定，从立法角度给予大数

据时代的隐私权保护以保障，从而使个人信息权益在网络空间也能得到充分的保护。下表为美国与个人信息保护相关法律的部分列举，见表 5-1：

表 5-1 美国与个人信息保护相关法律的部分列举

Table 5-1 Some of the laws related to the protection of personal information in the United States

1	1974 年	《隐私权法》	该法是美国有关公民隐私保护法中最基本、最重要的一部法律，其中有关保护公民个人记录的规定，在当今时代仍然在使用。
2	1986 年	《电子通信隐私法》	该法明确指出，法律保护涉及公民的以数字形式存在的隐私信息。此外，法律明确禁止黑客入侵获取信息的不法行为。
3	2010 年 7 月	《网络空间身份信任国家战略》	明确规定网络服务提供商在什么情形下可以收集用户信息，如何收集用户信息，收集什么样的信息以及如何管理和使用所收集的信息等。
4	2012 年 12 月	经修订的《儿童在线隐私保护法》	该法将保护扩展到新的领域，13 岁以下儿童在社交网络和智能手机的使用过程中，也会留存隐私信息，如照片、视频、地理位置等，该法要求网站和网络提供商在收集其信息时要获得其父母的同意认可。
5	2013 年 5 月	《应用隐私、保护和安全法案》	只有在征得用户同意并有能力保护所收集的数据时，移动应用开发者才能进行个人数据的收集。当用户不再使用应用程序时，可以随时要求开发人员停止收集并删除已收集的个人数据。

（2）行业自律

在美国行业自律已经成为一种社会文化，融入人们的日常行为方式。美国很早便倡导建立行业自律模式，当前美国的自律机制已相当发达，美国人的自律已经融入他们所追求的自由之中。[71]政府对网络服务提供商及运营商会采取相对宽松的政策，以此实现在激励其发展的同时引导他们建立自己行业内部的自律机制。通过运用企业的自我监管，自我约束以及行业协会的监督，对个人信息安全提供保障。在克林顿执政期间就已经认识到了行业自律的益处，号召充分利用行业自律来保护个人隐私。为了响应克林顿政府对行业自律的呼吁，许多行业组织都自发建立了保护个人信息的指导方针以响应政府号召。例如，银行业为了响应号召，通过银行家圆桌会议（Bankers Roundtable）设立了行业自律的指南，为银行业成员如何保护消费者隐私提供了一些明确的建议：消费者有隐私保护的需求这一点必须明确，要确保所收集、使用和保存的信息的准确性并减少员工的信息访问机会、通过确定的安全程序保护信息、限制账户信息的披露、在银行与第三方的业务中确保消费者隐私并把隐私政策充分向消费者公开。[72]

此外，在美国，拥有类似网络业务的个人之间存在自发的联盟，一些联盟将为他们所负责的网络业务设定一定的行业标准，这是最有意义的。这些指导方针是由一个名为“在线隐私联盟”的组织制定的。该联盟由大约由 80 个独立个体

在 1998 年夏天成立，他们为互联网开发了一个在线隐私指南，互联网上的个人身份信息可以受到行业的保护和监管。但该指导文件依靠的是同盟成员的自觉并不是联盟的监督，同时也为相关个体制定自己适合的用户个人信息保护指南提供了理论参考。

（3）设置专门的数据监管机构

美国有专门的政府网络监管的主管部门，即通讯委员会。其主要职责包括：当对网络监管权的划分有争议时，其有权制定相关法律解决争议；互联网具体监管工作的执行由其进行职权划分。在专业管理机构上则有基础设施保护委员会，负责监督网络基础设施建设，统筹协调网络监管工作及网络信息系统的更新、升级及技术防护。

5.1.2 欧盟移动互联网个人信息保护的经验

（1） 系统立法

1981 年，欧盟通过了《有关个人数据自动化处理之个人保护公约》，其对分析和处理个人数据的行为进行了具体规定，要充分尊重数据当事人的权利，与此同时还要采取措施保护个人数据免遭泄露。

此后，欧盟又于 1995 年颁布《个人数据保护指令》，这是其在数据保护方面的专门性立法，其中不仅对权利和义务进行了说明，特别是数据收集者应承担的部分作了明确说明，还对什么是数据保护的根本原则进行了解释说明。并且在指令中还指出要采取激励手段，使个人数据在欧盟成员国内部实现自由交换、传递，但要完全确保数据的安全性。除此之外该指令提出了几项基本规范，对如何处理所收集的个人数据进行了合理合法的指导。这对各成员国在个人数据保护立法上提供了借鉴，单个成员国制定的国内法只能比《个人数据保护指令》的要求更高，因为其是欧盟个人数据保护的基本法，各成员国要充分尊重基本法的法律权威。

任何法律都具有时代的印记，随着时代的发展，《个人数据保护指令》的相关条款已不能适应大数据、移动互联网等新兴领域对个人数据保护的要求，已经跟不上新时期的脚步，在个人数据保护领域的作用已大不如前，规制作用大大减弱。因此，在 2012 年《欧盟数据保护规则（草案）》正式由欧盟委员会发布，此草案实际上是根据新时期的要求对原《个人数据保护指令》进行修订，并最终将其取代，如果最终该草案被通过成为正式法律，那么其将会正式取代《个人数据保护指令》成为各成员国更新自己国内法的基本大纲。从总体上来看草案主要在以下几个方面发生了变动：法律适用范围、惩罚力度、监管机构设立及其职权划分、取得授权许可、告知及数据删除义务的履行等方面较之前的规定都发生了变化。最终各成员国都要按照这些变动进行自身个人数据保护标准的更新，最终

实现与草案的相关规定相统一。

总体来说，在个人数据保护方面，欧盟的系统立法非常全面，与美国的分散立法方式有很大的不同。此外，欧盟为了引导成员国设立适合自己个人数据保护的专项立法，其在立法准则方面作了统一规定，在其引导下多数成员国都顺利开展个人数据保护法的制定，例如德国、瑞典、西班牙等都在遵守欧盟立法准则的前提下设立了自己的个人数据保护法。这些法律是各成员国在个人数据保护方面的法律依据，为相关政府机构顺利开展个人数据保护工作奠定了基础。

（2）设置数据监管主体

为了保护个人信息，欧盟在 2001 年任命了一些负责此事的特别专员，他们有权监督欧盟的各相关机构和组织，时刻以个人隐私保护为工作重心。时刻提醒所有与保护个人信息相关的机构无论是开展业务时，还是其他任何时刻，都必须尽最大的努力来确保公民的信息安全，就是特别专员存在的主要意义。同时，针对数据处理的各环节，例如信息收集、利用、保存、删除或销毁数据等，欧盟都针对这些行为制定了严格的保密条例，此外，涉及公民种族或宗教信仰、政治观点、或工会成员资格的个人数据，任何欧盟组织和机构都无权处理。根据《数据保护指令》的规定设立了通常被称为“第 29 条工作组”或“数据保护工作组”的保护个人信息的专项工作组，2009 年，他们就曾分别致信三大搜索巨头：谷歌、雅虎和微软，其指出对于三大搜索引擎来说，都要缩短用户搜索数据的保留时间且必须少于原定的 6 个月，以此来保证用户个人数据的安全性。

5.1.3 日本移动互联网个人信息保护的经验

（1）统分结合的法律保护模式

日本为了制定与个人信息保护有关的法律法规，对美国在与互联网相关的各领域分散立法的形式以及欧盟采取统一立法的形式都进行了充分的研究与分析，并在分析的基础上进行了学习借鉴，形成了兼具欧美特点的立法模式。例如，在 1998 年，其在学习美国《隐私权法》的基础上，加以本土化的转变，充分结合自己国情，颁布实施了《关于对行政机关持有的计算机处理的个人信息加以保护的法律》，充分吸取了美国隐私法的精髓。此法在个人信息保护方面，对政府机关工作人员的行为也作出了规定，只要是从事与个人隐私信息相关的数据处理行为，也必须严格遵守个人信息保护原则，以求通过此项规定对降低侵犯个人信息不法行为的发生率发挥一定作用。其次，国际化进程的加快也大大促进了各国的贸易往来，对日本来说，欧盟是其最重要的贸易合作伙伴之一，在对欧盟《个人数据保护指令》进行借鉴的基础上，在 2000 年日本出台了《关于个人信息保护基本法制的大纲》，其在形式上与欧盟立法有极大的相通之处，不仅实现了立法保护个人信息的目的，更加推动了与欧盟贸易合作关系的深入发展。除以上提到

的法律，日本为保护个人信息安全，还逐步颁布了许多法律，具体见下表 5-2：

表 5-2 日本与个人信息保护相关法律的部分列举

Table 5-2 Part of Japan's law on personal information protection

1	2001 年 3 月	《关于个人信息保护的法律案》	个人信息保护法律改革的起点
2	2003 年 3 月	个人信息保护“五法案”[①]	个人信息保护法制系统完善过程中的奠基之作。其中明确规定，法律保护任何与识别个体有关的个人信息；无论何种情况下要想进行个人信息收集行为，首先要做的准备工作就是向信息主体征求是否可以授权；法律保护一些在大数据背景下实现电子化的与个人有关的特殊信息（如数字符号）等。[73]
3	2003 年 5 月	《个人信息保护法》	对“个人信息”、“个人信息数据库”、“个人信息处理者”、“个人数据”、“所持有之个人数据”、“本人”等名词进行了明确定义。同时，明确规定了国家和地方公共组织在保护个人信息方面的责任以及个人信息处理运营商的义务，在保障个人信息安全的前提下，应提前预防和遏制滥用个人信息等违法行为。
4	2011 年 11 月	修订《电信业个人信息保护条例》	对在何种情形下可以获取、使用或者向其他方提供个人位置信息进行了全新及详细的规定。[74]
5	2014 年 6 月	修订《个人信息保护法》	建议企业可以提供和使用的信息,例如：无法推断出特定个人的信息。但“私人信息”,如种族、信仰和社会身份不得提供；与此同时,建议将与身体特征相关信息，如面部识别数据，也纳入到个人信息的保护范围。

（2）设立信息公开与个人信息保护委员会

首先，在 1980 日本设立个人信息保护研究所，其在保护个人网络隐私问题上提出了一些极具指向性的要求，具体有以下几点要求：第一，所收集的个人信息必须要用于已向用户告知的用途，不得超范围使用。第二，严格按照法律法规关于收集范围等相关规定进行个人信息的收集工作。第三，有关部门的职权要进行明确划分，避免职权交叉。第四，个人对被收集了哪些信息以及使用目的都有权知晓，必要时还可以要求对信息进行核对。1998 年，有关法律中提议建立一个组织，当个人与公共机构在涉及个人信息上的问题上产生争议时，有权进行协调的个人信息保护审查委员会组织，但其对防范个人信息侵害行为的作用很有限，因为其并不具备实际意义上的监督权及执行权，可能仅仅属于咨询机构的范畴。1999 年，根据《行政机关信息公开法》的提议，并根据相关规定设立了信

[①] 个人信息保护“五法案”指《个人信息保护法》、《信息公开、个人信息保护审查会设置法》、《独立行政法人个人信息保护法》、《行政机关个人信息保护法》及《行政机关个人信息保护法等施行准备法》

息公开审查委员会。2005 年，《信息公开、个人信息保护审查会设置法》中提议将早先设立的相关的专职机构进行合并，信息公开与个人信息保护委员会由此应运而生。但该机构性质并未发生太大转变，在法律上依然不具备强制性的权利。

（3）相关配套机制的施行

行业自律可以对政府在个人信息保护方面的监管工作起到很好的辅助作用，更能帮助政府实现相关的监管目标。日本政府为了更好的实现个人信息保护目标，提高管制政策的灵活性，促进各行各业实现高速健康发展的同时又能充分尊重个人信息权益，提倡与互联网相关的各行业对自己的行业情况进行分析，基于行业现实及需求，建立高度适应性的行业的个人信息保护规则。1999 年，日本颁布了《个人信息保护管理体系要求事项》，其中为了提高公民对行业机构可信度的辨别能力，会为相关机构颁发独特的隐私认证标志（P-mark 认证），但只提供给保护个人信息得力的机构，以此来激励各行各业竞相提高个人信息保护意识。此外，在 2001 年引入了“安全管理系统评估制度”，该系统与国际上通行的标准相呼应，以对各行业的信息管理行为进行相对严格的规范。

5.2 国外移动互联网个人信息保护的特点比较与启示（Comparison and Enlightenment of Personal Information Protection on Mobile Internet Abroad）

5.2.1 国外移动互联网个人信息保护特点比较

下表 5-3 为美国、欧盟、日本三国个人信息保护政府监管的特点：

表 5-3 美国、欧盟、日本三国个人信息保护政府监管的特点

Table 5-3 American, European Union, Japan three countries personal information protection government supervision characteristic

美国	欧盟	日本
为了促进贸易自由的发展，美国避免了政府的过度干预，实行行业自律为主的监管模式，以分散的立法起辅助作用。但是美国也对行业自律行为进行规制，引导其良性发展，从而实现更好的保护个人隐私。	欧盟对个人数据的保护，在立法方面，与美国分散立法模式恰恰相反，采取系统立法模式。各成员国根据《欧盟个人数据保护指令》制定自己国内的个人数据保护指令，《欧盟个人数据保护指令》主要起到规范指导作用。此外《欧盟个人数据保护指令》还要求各成员国建立统一的监管机构。监管机构的职责主要包括：对侵犯个人数据的行为进行处罚，披露有关机构的违法行为，使公民享有知情权，从全方位保护个人信息安全。	从自身的经济和社会发展状况以及信息产业的发展出发，日本同时学习借鉴欧美的在保护个人信息方面的立法特点，最终形成统分结合的立法模式。日本在个人信息保护方面既有全国性的个人信息保护法，而且也倡导各地区行业按照各自现实情况，制定自己地区和行业内部保护个人信息的法规。此外，日本为解决与个人信息相关的分歧问题还设立了个人信息保护委员会。但该委员会的性质是咨询性机构，并不具备行政上的强制力。日本也鼓励各行各业建立了适当的行业自律规则。

5.2.2 国外移动互联网个人信息保护的启示

（1）立法的启示

与美国、欧盟、日本相比，我国在立法方面还存在许多不完善的地方。当前我国在一些法律法规中都能看到与个人信息保护有关的条文、规定，例如：《刑法》、《消费者权益保护法》、《中华人民共和国电信条例》等法律法规中都有所涉及，但惟独还未设立一部特别法来保护个人信息。然而缺乏个人信息保护的特别法，仅靠其他相关法律法规，并不能对侵犯个人信息的违法行为起到很好的规制作用，相应的也无法实现保障信息主体权益的目的。更何况，法律中现有的与个人信息保护有关的法律条文，大多是为了应对传统互联网时期的个人信息保护问题，而如今使用移动互联网的用户群体正逐步攀升，个人信息泄露问题在移动互联网环境下变得更为严峻，用现有法律条文去应对移动互联网时代下个人信息泄露问题，难免会遭遇适应性、时效性不足等一系列问题。

此外，美国为了保护个人信息在一些特别领域会进行专门立法的做法，我们也可以进行学习借鉴。就如美国为了保护 13 岁以下的儿童群体的线上隐私，专门颁布了《儿童在线隐私保护法案》，足以看出美国对个人隐私的重视程度。而我国在这方面还未开展相关的立法工作，也未对用户群进行年龄划分以便进行特别保护。

在现实生活中，有些人游走在法律边缘，钻法律漏洞的行为时有发生，很大一部分原因是由于个人信息保护相关法律法规的更新速度过慢，远远满足不了移动互联网时期个人信息保护的要求。所以，我国在立法时，在遵循我国国情的基础上，学习借鉴美国、欧盟、日本的立法形式，制定法案时也要兼顾法律的前瞻性、广泛性和适用性。

（2）管理体制的启示

参考美国、欧盟等设立的专职机构，我国也可以学习他们的做法，设立一个专门机构，统筹领导全国范围内在移动互联网个人信息泄露问题方面的政府监管工作。省市范围内可以下设各自的网络个人信息监管小组，承担自己区域内的监管职责，但其也应接受全国性专门监管机构的监督，形成统一协调的监管体制，改变多部门职权交叉，管理混乱的局面。

（3）行业自律的启示

尽管政府主导的移动互联网个人信息监管模式能够起到监管效果，但并不能从根本上解决个人信息泄露问题，行业内部的不重视或者过于追逐经济利益是导致个人信息泄露的主要原因之一。更何况当今网络世界瞬息万变，网络技术不断发展，单纯依靠政府力量来管理网络世界中的个人信息泄露问题是远远不够的，所以美国、欧盟和日本都很重视对行业自律的积极作用加以利用，美国更是倡导

要充分利用行业自律模式。美国的行业自律模式已融入社会风气，网络监管工作的重心一直以行业自律为主，行业自律规则已成为建立和完善网络监管体系的重要组成部分。美国行业协会的职权所涉范围比较广泛，例如行业自律规则的制定、对公众的投诉进行协调处理、进行个人信息保护有关的宣传教育工作等等，形成有效的行业监管，政府对行业自律加以引导。我国的自律模式与美国、日本相比显得非常简单，还处于起步阶段，目前，只有少数的自律协会但也发挥不了什么实际作用，而且仅有少部分的互联网企业加入其中。在行业指引方面，中国互联网协会发布了《中国互联网行业自律公约》和《文明上网自律公约》等，是当前我国为数不多的行业自律公约，但这些公约类文件实操性不强，无法真正发挥作用，且行业内的公共责任意识还不足。在设立认证机制上，我国目前还未开展与此相关的工作。

6 完善移动互联网个人信息泄露政府监管的对策

6 Measures to Improve the Government Supervision of Personal Information Disclosure on Mobile Internet

6.1 健全相关法律法规(Sound Relevant Laws and Regulations)

6.1.1 加快网络立法进程

长期以来，我国在互联网监管领域，拥有监管权的部门众多，在监管模式上属于多部门联合监管，这也是传统互联网时期的监管方式了，如今面对移动互联网高速发展的趋势，依然延续传统互联网时期的监管模式，各部门依然各自为阵，各自依据各部门的部门规章进行监管，相关部门协调力不足，且明显缺乏监管依据。移动互联网所涉及的行业众多，涉及我们生活的方方面面，但是我国在移动互联网领域还缺少一部全覆盖的基本法，立法进程相对于移动互联网领域面临的一些新问题的急需解决的现状来说还比较落后。实际上，在 2005 年就已经探讨设立《电信法》，甚至已经进入了正式的立法议程，然而时至今日，《电信法》仍然止步不前。当然，在移动互联网监管领域我国也取得了一些不小的成就，例如：2013 年 11 月工信部实施的《关于加强移动智能终端管理的通知》，其中对智能终端制造企业提出了一些行为规范，要求其不能在移动终端提前安装某些应用软件，希望通过严格管理智能终端的途径来保护使用者的个人信息安全，不得不承认这推动我国在网络监管立法进程迈出了一大步。但是，归根结底，我国的立法现状是涉及移动互联网行业管制的正式法律太少，大多数都表现为政策、通知、意见，但归根结底这都不属于真正意义上的法律，并不具备法律的强制性，因此，大力加快移动互联网领域的立法进程，是迫在眉睫的。因此，全国人大及其常委可以对近些年来涉及移动互联网监管领域的法律法规、条例、部门规章、地方性法规以及行业自律公约进行整合，正式颁布覆盖面广且能统筹全局的《电信法》，站在全局的高度确保立法的前瞻性和可操作性。

6.1.2 完善个人信息保护专门立法

近年来，几乎在每个人身上都或多或少的遇到过信息泄露的情况，且发生频率非常高，甚至给个人带来难以挽回的严重后果，随之而来的是一系列的信息泄露侵权所引发的纠纷案件，此类案件要想处理也非常困难，移动互联网时代人们的一大需求就是个人信息保护。个人信息侵权案件之所以难以解决，最主要的原

因就是在执行过程中缺少监管依据，因此政府要积极推动建立个人信息保护的立法进程，不断完善相关法律法规，更好完善监管依据，通过立法途径来维护个人信息权。从上文对欧美等国家和地区的分析及国际上相关数据统计，可知全球范围内在个人信息保护立法领域相对比较完善的国家已有将近一百多个。但我国的现实情况是，虽然政府也在不断努力尽可能地完善与互联网个人信息保护相关的法律法规，但大都是些有关的法律条文，零散的分布在一些现有法律法规中，但这也恰恰从另一个层面反映出我国个人信息立法保护方面的一大缺陷——太过分散、系统性不足，法律规定上存在交叉，缺乏专业性、精确性以及可操作性，因此在监督实践过程中依然存在“无法可依”的问题。齐爱民教授曾指出：“个人信息保护法的效力层次分为三层，效力从高到低分别是保护个人信息的特别法、保护个人信息的普通法、民法和行政法等基本法”。[75]从上述分析中可以看出，在一些普通法和基本法中都有一些涉及该领域的法律条文，这意味着保护个人信息的有效性很低。因此，为了最大限度的发挥法律的作用，从立法角度保护公民的个人信息，急需出台一部《个人信息保护法》的特别法。

早在 2003 年《个人信息保护法》就已经开始起草，但由于移动互联网时期个人信息电子化的普及并且情形越来越复杂，这在一定程度上也间接导致了相关立法进程放缓，《个人信息保护法》至今都没有被正式颁布。当今，移动互联网对社会有着巨大的影响力，个人信息安全事关社会和谐、稳定、有序发展。政府可以充分学习借鉴美国、欧盟、日本等国家在该领域立法模式上的可取之处，并在学习借鉴的基础上与我国国情及个人信息保护的立法需求综合考量，早日将《个人信息保护法》提上立法进程，推动其早日出台，以此为移动互联网环境下个人信息泄露政府监管工作的进行提供明确、有效的监管依据，为个人信息提供法律保障，使相关部门在监管工作中真正实现有法可依。

6.2 进一步完善监管机制(Further Improve the Regulatory Framework)

6.2.1 弥补职能缺位，成立专门的职能部门

当前，涉及个人信息保护的监管权分散在多个部门，还未设立专门机构来负责个人信息保护所面临的问题，依然沿用长久以来的多部门联合监管模式，但这也相应的带来了职权交叉、监管过程中互相推诿导致监管不力等问题。与美国、欧盟、日本等国家和地区相比，他们已经建立相关专职机构来解决该领域的问题，针对我国的监管现状来说，建立一个个人信息保护专职机构，以更好的应对个人信息泄露发生在移动互联网环境下所带来的新的监管需求，已变得非常迫切。

设立个人信息监管专职机构，可以有效的缓解当前许多迫在眉睫的问题。首

先，现阶段政府在个人信息保护上还未能充分发挥统筹作用，相关职能部门只是被动地应对个人信息泄露问题，各部门对各自的权利义务并不明确，由此也引发了许多弊端，在个人信息泄露问题上只能发挥很小的监管作用。设立个人信息监管专职机构，可以集个人信息保护问题与一身，方便理清相关职权，统一安排相关部门的工作，提高监管效率从而更好地保护个人信息权益。此外，还有利于培养网络监管专业人才，提升监管工作人员的专业度；其次，当前一旦发生侵犯个人信息违法行为所引发的纠纷案件，公众除了去公安部门报案，根本不知道其他的维权途径，但传统的公安部门在应对移动互联网环境下发生的个人信息泄露问题给信息主体带来损害的问题上，并不专业，最终导致维权失败。而个人信息保护专职机构的设立，就会使个人明确维权机关，提高维权成功的概率，降低维权成本，提高维权意识，对政府的信任感也会提升；第三，设立个人信息保护专职机构，由于在针对性及专业性上都得到了大幅提升，由其来解决个人信息泄露所带来的一系列问题，监管效果也一定能实现大幅提升，同时，它还可以带头与其他部门（例如公共安全和工业信息部门）联合执法，以打击从事个人信息交易的个人和团体。

简而言之，为了满足新时期的需求，政府要提高对新环境的适应能力，顺势而为，加快推动个人信息保护专职机构的设立，既满足移动互联网背景下公众对个人信息保护的需求，又能更好地履行个人信息泄露政府监管职责。

6.2.2 建立分级监管体系

移动互联网涉及许多不同种类的运营主体，针对所涉及的不同种类的监管主体，在监管标准上不能一刀切，应制定适用于移动互联网全领域的个人信息安全监管标准，该标准要具有高度的灵活应和针对性。首先，最重要的就是对各监管对象（即移动互联网各运营主体，例如运营商、运营服务提供商）进行分类分级监管，因为其在服务类型和用户规模上都有很大的差距，因此不同的类型要制定不同的监管标准和要求，增强监管过程的灵活度。

6.2.3 建立完善登记、举报和反馈制度

第一，应全面落实网络实名制。当今互联网的发展现状以及移动终端的全面普及，为了更好的开展个人信息监管工作，网络实名制的推进势在必行。首先，所有使用互联网的人（个人、企业、社会团体、政府机关等等）原则上都应进行实名登记。为了充分落实可以实行登记、备案的双保险制，既要到电信部门登记也要到公安机关备案。其次，手机卡实名制已基本全面落实，但如今移动互联网运营商不断开拓业务范围，例如：腾讯网卡、阿里网卡等各种各样的移动网卡开始泛滥，甚至一人名下可以有多张不同类型的网卡。可以说移动网卡目前的管理

异常混乱，需要建立统一的移动网卡登记制度，进行严格管理。再次，应全面落实代理服务器实名登记政策。代理服务器（Proxy Server）严格意义上来说相当于一个中介，是私人网络和网络提供商联系的媒介，在他的帮助下实现了网络信息的中转，从而网络使用者能够顺利获取所需要的信息。但通过其获取的信息必须是合法信息，在获取过程中还要进行相应的控制和登记。此外代理服务器的作用还包括：提高网速、共享网络、充当防火墙、登陆国外或国内限制网站、隐藏真实 IP 等，其本应发挥积极作用，为公众生活带来便利。但却被黑客等不法分子找到部分功能（隐藏 IP）的漏洞并进行不合理利用，很多黑客会利用相关功能对计算机进行攻击，以获取其中留存的个人信息，进行违法犯罪活动。当前对代理服务器的下载和使用并没有特别的规定，只要是互联网用户都可以自由下载，一旦发生侵犯个人信息的违法犯罪活动，这就在一定程度上导致了嫌疑人难确定。若代理服务器提供商也能建立落实实名登记政策，要想下载使用必须进行登记，那么不仅可以震慑不法分子减少不法行为的发生，即使发生了不法行为后期的追责也会相对容易不少，可以省去很多不必要的工作。最后，互联网访问时也应进行实名登记。当前，我国移动互联网软件应用实名制方面已经取得了一些成就，例如：各大银行的自助 APP、12306 网站、微信、支付宝、淘宝等 APP。总而言之，网络实名制不仅可以规范用户的网络行为，还可以在一定程度上减少侵犯个人信息行为的发生。其实早在 2007 年韩国就已经要求使用真实身份在网上进行登记注册、发表言论等行为，逐步落实网络实名制。

第二，完善举报制度。首先，可以建立专门受理举报的机构。根据我国移动互联网个人信息泄露的监管现状，为了更好的保护个人信息，政府职能部门可以设立专门受理举报的机构，也应要求相关的网络服务提供商参考政府相关规章制度建立相同或者相似的机构。目前，公安部已经设立了“网络违法犯罪举报网站”，该网站专门用于接受网民举报，但在网站管理制度上还存在一些需要完善的地方，例如：当前举报受理流程和处理期限还不明确、举报方和受理方的权利义务还未进行明确的划分，举报网站必须重视这些问题并不断改进。其次，可以建立奖惩机制辅助举报网站工作的开展，奖励举报者的同时也要辨别恶意举报者并进行相应处罚。

第三，推动建立互联网使用轨迹的报告反馈制度。报告反馈制度简言之就是网络服务提供商应当如实记录互联网用户的网络行为轨迹，出现异常时及时将异常信息反馈给用户，用户可以在第一时间知晓情况，尽可能避免遭受侵害。政府职能部门在移动互联网个人信息泄露监管方面该模式也同样使用。形形色色的移动互联网平台、APP，他们对于每个用户的使用痕迹都会时时进行记录，向用户反馈这一功能并不难实现。例如：腾讯 QQ、微信账号如果被盗取并被异地登录

时，腾讯的系统就会第一时间向用户发送报告，用户就能第一时间知晓，在很大程度上对保护用户个人信息提供帮助，政府部门在个人信息保护过程中可以对该模式学习借鉴并加以合理的利用。

6.3 强化信息安全宣传与教育的功能(Strengthening the Function of Information Security Publicity and Education)

6.3.1 政府加强宣传，提升个人信息保护意识

加强宣传，提升移动互联网用户自身意识，从源头对个人信息提供保护。政府在监管过程中应重视用户自身的作用，从用户本身出发，减少侵犯个人信息行为的发生。政府要时刻利用各种手段、方式尽可能全面的普及和宣传个人信息保护方面的相关知识，但宣传普及手段也要顺应时代变化，跟随现实情况进行相应的转变及创新，尽可能的通俗易懂，使用户能够快速掌握并加以利用。国家可以在文化建设过程中增设个人信息安全保护宣传项目，以保证相关宣传工作的执行和落实。具体做法可以概括为以下两个方面：

一方面政府职能部门的宣传工作以线上、线下同步开展的方式进行，实现多元化宣传。线上可以充分利用时下传播途径最广、速度最快的各种新兴媒介，例如可以通过开设官方微信公众号、官方微博账号、政府部门官方网站等方式进行宣传，但也应注意通过此类方式进行宣传，必须由专人进行管理，提高宣传效率和有效性。线下可以通过发放个人信息保护宣传册、电视广告、在电视节目中穿插小节目、宣传视频等多种途径，充分宣传如何保护好自己的个人信息，要注意的是在发放宣传手册时要尽可能的实现全覆盖，可以借助一些地区委员会、学校、企业等社会各方的力量。通过以上种种方式向公众传达在移动互联网使用过程中需要填写个人信息时，要明确什么样的信息可以填，什么样的信息不可以填，提高用户的辨别意识和能力，以此从自身出发更好的保护个人信息。

另一方面宣传的内容要要简洁明确。在宣传过程中要把个人使用网络的过程中收集个人信息的常见方式以及保护个人信息的防范措施和注意事项向公众传达。比如：告知用户在使用浏览器等工具进行网页浏览和搜索时可以开启无痕模式或者关闭 cookies（信息记录程序），因为一旦我们的浏览轨迹被收集并加以分析，我们将面临的就是铺天盖地的推销广告、垃圾信息等，从而影响我们的正常的搜索活动，一不小心还会上当受骗造成经济损失；此外在使用各种 APP 时要避免向其开放过多的权限，在授权时要深思熟虑，辨别是否有必要向软件提供者进行授权，在可以不授权的情况下最好不要授权。而且在使用需要提交个人信息的 APP 时，例如淘宝、京东等购物软件，微信等社交软件尽可能不要填写过于详细的个人信息，只提供一些必要信息即可，尽可能减少个人信息被收集；对

一些不明来源的链接不能点击，因为很可能是钓鱼网站，一旦点击我们的个人信息很可能被恶意收集；在自己的个人信息被泄露时，不能保持沉默要敢于维权。

政府部门通过以上多途径、有针对性的个人信息保护宣传工作，让公众无论在学习、工作、生活中时时刻刻都能接触到个人信息保护宣传工作，逐步提高个人的信息保护意识与能力。

6.3.2 扩大信息安全教育范围

政府要充分发挥教育的力量，实现信息安全教育的全覆盖，相关政府职能部门的工作人员、网络服务提供商等企业员工、社会公众都应涵盖在信息安全教育的范围内，提高全社会个人信息保护知识的水平。

首先，对相关政府部门的工作人员，要开展保护公民个人信息安全的教育。不仅要对其进行素质教育，也应进行知识技能教育，提高其职业素养的同时也能同步保证监管技能的提升。首先从工作人员的思想教育着手提高其监管工作中的责任意识以及保护公众个人信息的意识。此外，为了使相关监管人员的监管技能能跟上移动互联网时代下个人信息保护的需要，可以定期开展有关信息安全保护、监管技能的培训、讲座、论坛等等，可以拿出相关职能部门在网络个人信息侵权案件中大获全胜的案例拿出来讲解，总结监管成功的经验并加以运用，从实际工作的经验出发全面提高监管技能。

其次，对移动互联网各提供商的员工开展保护用户个人信息的教育，让员工意识到保护用户个人信息的重要性。政府部门要向企业灌输加强员工信息保护意识和技能的重要性，通过政府部门的督促逐步引导企业树立保护用户个人信息的责任感。具体做法可以参照相关政府部门的做法和规章要求，也可以让企业结合自身情况设立其独有的培训机制。引导移动互联网提供商从企业内部做起，严格遵守保密原则，合理合规收集、使用用户个人信息。避免提供商内部出现侵犯个人信息的现象或因自身系统脆弱轻易被黑客攻击导致泄漏用户的个人信息。

最后，在基础教育中加入信息安全教育，从小就要向公众灌输个人信息保护意识。由于移动互联网的覆盖，即使是小学生在学习生活中也不可避免的要使用手机等移动终端，可见移动互联网的用户群已经开始向青少年延伸。其实不管是青少年还是一些比较年长的群体，由于年龄阅历及时代背景的关系，相对而言其不论在防范知识还是技能上都比较欠缺，面对当今侵犯个人信息的途径多样化的形势，他们更可能会遭受侵犯个人信息的事件。相关监管部门可以利用教育教学的强大力量，与教育部门合作，在九年义务教育的课程内，专门开设与信息安全基础知识和基本保护技能相关的课程，从小便开始向青少年普及相关知识，尽可能实现提高全民信息安全意识的目标。

6.4 引导规定明确的行业自律规则(Guiding Clear Industry Self-Regulation)

6.4.1 明确行业监管主体

要想充分发挥行业自律对移动互联网个人信息泄露政府监管的辅助作用，首先要明确行业监管主体，设立一个统一的行业自律机构，为政府监管工作注入新的活力。移动互联网所涉及领域众多，可以说现实生活中的各行各业都开始线上发展，由于行业属性不同，在用户个人信息保护方面不能一刀切，在尊重法律权威的基础上，政府需要充分调动行业自我监管的作用，但要想利用行业监管的辅助作用，需要一个统一的行业监管机构从中进行协调，才能顺利展开相关工作。在现实生活中，虽然已经设立了中国互联网协会，但由于监管权有限，并未起到太大的作业。在以后的实践工作中，可以下放权利，使中国互联网协会具备一定的主观能动性及合理的监管权或者重新设立一个全新的行业监管协会，赋予其收集移动互联网各行各业对保护用户信息的见解以及各行业运营过程中已发生过的泄露个人信息的典型案例，集思广益又充分尊重现实情况的基础上制定统一的行业监管规则，并对相关规则的落实执行情况进行监督；此外在监管过程中如果遇到一些因专业性太强而难以应对的问题，此时也可以寻求专家的帮助，由其为我们提供专业性的建议。明确行业监管主体，代表行业与政府共同为个人信息提供保障，积极将行业内部的情况向政府相关职能部门反映，以更好地提供服务，加强从业者技术培训，减少行业内部发生个人信息泄露问题。

6.4.2 透明化个人信息的收集方式

与移动互联网有交集的行业在个人信息收集时，必须依法行事，按照法律法规中有关告知原则和保密原则的相关规定行事。必须合理合法的收集个人信息，并充分向用户传达收集个人信息的内容、途径、适用范围，在经过用户授权后方可进行收集，未取得用户的授权严禁私自收集，不得利用“霸王条款”，不得违反法律法规。在收集用户个人信息的过程中，还应充分尊重保密原则，严格按照取得用户授权时所出具的保密协议有关条款的规定，不得作出任何违反保密条款的侵犯个人信息的不法行为。监管部门也可以针对各行业设定一个收集个人数据的最大规模，从根本上防止非法获取个人信息行为的发生。

6.4.3 加快制定行业内部监管细则

我国的移动互联网监管政府处于主导地位，行业自律机制处于初始阶段，相关的行业自律章程和公约的实际操作性不强，在实践过程中存在很多问题，行业内部监管细则的制定事关行业自律机制的不断优化。移动互联网各行业首先要开展的一项比较重要的工作就是提高行业监管规则的可操作性，对其进行细化。相

对于美国、欧盟等国家来说，我国的自律模式还很不成熟，因此政府需要引导移动互联网各行各业完善行业自律机制，细化行业监管规则，推进行业自律组织积极探索全新的行业自律模式，帮助政府落实监管职能。

6.5 加大技术投入，成立高素质监管队伍(Increase Technical Input and Set Up High-quality Supervision Team)

6.5.1 政府部门加大技术投入

移动互联网个人信息泄露给人们的日常生活带来了一系列不好的连锁反应，更有甚者因个人信息被泄露，财产乃至生命都受到了威胁，社会秩序也遭遇了不小的挑战，阻碍了社会进步。移动互联网环境下的个人信息泄露问题，由于存在范围广、程度深等特点，相比传统互联网时期，监管起来难度更大，对政府监管技术提出了更高的要求。现阶段政府相关职能部门的监管技术还跟不上网络的发展步伐，政府应该加大网络监管领域的技术投入，增强对网络的驾驭能力，运用技术手段来更好的应对个人信息泄露问题，提高监管效率和效果。

政府职能部门要充分发挥资源配置的作用，增加监管技术领域、信息科技研发行业的人力、物力、财力的投入力度，加快监管部门所运用的的监管技术的提高以及监管设备的更新换代，加快个人信息政府监管领域的稳定持续发展。此外，政府部门可以对保障个人信息安全成效显著、贡献较大的行业给予一定的优惠政策，例如税收减免等，加快个人信息保护核心技术的研发力度，改变当前过于依赖美国等技术强国的现状，把命运掌握在自己手中，设计出更加安全高效的个人信息保护系统，从源头上缓解个人信息泄露高发生率的情况。因此政府相关职能部门在充分考虑移动互联网环境下个人信息泄露政府监管的现状，明析信息技术研发领域的方向，并与个人信息保障的监管技术要求相契合，推动我国信息保护领域监管技术的有序发展。

6.5.2 成立专业的网络监管团队

要实现科学技术向生产力的转变必不可少的一项因素就是人才，政府必须引进与移动互联网监管环境相匹配的监管技术人才，全力开展专业人才队伍建设，打造一支兼具网络技术水平和管理水平的一流团队。从专业人才的角度确保专业技术的提升，最终运用先进的技术手段来更好地保障个人信息的安全。人才是技术的载体，只有拥有高素质、高技能的监管队伍，为个人数据监管和安全防护提供强有力的技术支持，最终才能为个人信息安全保驾护航。

7 结语

7 Conclusions

移动互联网的快速发展，让我们的日常生活变得便利了许多。现如今，无论相距多远，无论在地球的哪一端，即使隔着千山万水，只要你所在的地方有网络，利用移动终端就可以与他人实现时时沟通交流。此外许多日常生活，借着移动互联网都已实现了网络化，例如：12306 订火车票、机票预订、酒店预订、美食预定、查天气等，日常生活所需基本都可以借助网络和移动端实现，生活的便利性较之前提升了不止一点点。但任何事物的出现可能都有两面性，互联网与移动智能终端相结合无论是从技术创新的角度来看还是大幅提高日常生活便利性的角度看，其益处都是不可否认的。但另一方面，他也给人们制造了一些新的麻烦，频繁爆发的用户个人信息泄露事件，越来越多的用户认识到移动互联网的应用就是一把双刃剑。当前的现实情况就是，无论个人信息保护措施得当与否，只要某一个环节处理不力，就可能出现个人信息泄露的问题。因此，在移动互联网的大环境下，如何保护用户个人信息免遭泄露，开始成为人们重点关注的问题。

文章正是基于对移动互联网发展现状的分析以及保护个人信息的需要，探讨移动互联网环境下的个人信息泄露问题，将二者结合起来进行分析探讨，选取了移动互联网中比较受人们关注以及对人们生活影响最为严重的问题之一着手，以个人信息泄露问题作为切入点，从政府监管的视角进行分析，论述政府如何更好地保护移动互联网上存在的用户个人信息。

文章首先对一些基本概念、基础理论进行了阐释，并建立了全文的分析框架，为进一步分析打下基础，此后进一步对当前我国移动互联网监管现状进行考量，分析我国移动互联网监管中存在的问题，特别是在涉及个人信息保护方面存在的问题。为了后文能够更具针对性的提出优化建议，更对政府监管的关键影响因素进行了详细分析，以求找出政府监管不力的原因，同时通过分析美国、欧盟、日本三国在个人信息保护方面的举措，并进行比较分析，总结出他们在个人信息保护方面的长处以及可供借鉴之处，方便我国在尊重现实国情的基础上对其进行学习借鉴，以便更好的为个人信息提供保障。

通过上文分析得出我国政府相关职能部门在监管过程中由于存在法律漏洞甚至法律真空，以至于实际工作过程中缺乏监管依据，导致监管工作难以进行；监管机构、行业自律机制相较于美国等国家存在一些不足的地方；监管技术落后，监管效果差等等问题，因此，本文也有针对性的对监管依据、监管机构、行业自律、文化教育、技术手段等各方面提出了完善对策。

笔者希望通过本文分析探讨，能够为解决移动互联网个人信息泄露政府监管

工作中存在问题的解决提供一些参考，希望政府能够针对监管现状有针对性的采取相应的措施，从而能够更好地完善政府职能，为公众提供公共服务，保护公众利益。由于笔者在理论水平、文献收集上还存在许多不足的地方，对内容的论证及表述上也存在着一些不恰当的地方，还有很多问题需要思考和探讨，希望老师、同学们多多指正。

参考文献

[1] 中国互联网协会,中国互联网络信息中心.《中国移动互联网发展报告(2018)》[EB/OL].https://baike.sogou.com/v175662630.htm?fromTitle=%E4%B8%AD%E5%9B%BD%E7%A7%BB%E5%8A%A8%E4%BA%92%E8%81%94%E7%BD%91%E5%8F%91%E5%B1%95%E6%8A%A5%E5%91%8A%282018%29.

[2] 中国互联网络信息中心.《第 42 次中国互联网络发展状况统计报告》[EB/OL].http://www.cac.gov.cn/2018-08/20/c_1123296882.htm.

[3] 中国青年政治学院互联网法治研究中心.封面智库.《中国个人信息安全和隐私保护报告(2016》[EB/OL].http://www.sohu.com/a/128010313_481893.

[4] Banisar D,Davies S.Global trends in privacy protection:An international survey of private ,data protection and surveillance laws and developments[J].Jouranl of Computer&Information Law,1999,18(1):3-111.

[5] 布兰代斯.译者徐爱国.哈佛法学评论：侵权法学精粹[M].北京：中国法律出版社.2005.12.

[6] 刘雅辉,张铁赢,靳小龙,程学旗.大数据时代的个人隐私保护[J].计算机研究与发展,2015(01)：229-247.

[7] 黄晓晓.社交网站隐私侵权及保护研究——基于个人信息与数据安全视角[J].今传媒,2016(01)：51-54.

[8] 关伟明.欧美个入数据保护制度及对我国的启示[D].广西:广西大学,2014.

[9] 赵衍.互联网时代的信息安全威胁——个人、组织与社会[M].北京:企业管理出版社,2013.

[10] Daniel J. Solove,Paul M, Schwart. Information Privacy Law[M]. Wolters Kluwer, 2009.

[11] 李皓.网络环境下个人信息泄露的理论分析及防范探讨[J].情报探索,2011(1).

[12] Bhasin M. Challenge of guarding online privacy:role of privacy seals,government regulations and technological solutions[J].Socio-Economic Problems & the State.2016,15 (2):85-104 .

[13] David Dunbar,Michael Proeve,Rachel Roberts. Problematic Internet Usage self-control dilemmas:The opposite effects of commitment and progress framing cues on perceived value of internet,academic and social behaviors[J].Computers in Human Behavior,2018,82:16-33.

[14] Carey Doberstein.Problematic Internet Usage self-control dilemmas:The opposite effects of commitment and progress framing cues on perceived value of internet,academic and social behaviors[J].Computers in Human Behavior,2018,82:16-33 .

[15] Roy I,Setty S T,kilzer A,et al.Airavat:Security and privacy for Map Reduce[c]//Proc of the 7th USENIXSymp on Network Systems Design and IMPLEMENTATION(NSDI).Berkeley,CA:USENIX Association,2010,297-312.

[16] Mowbray M,Pearson S,Shen Y.Enhancing privacy incloud computing viapolicy-based obfuscation[J].The Journal of Supercomputing,61(2):261-297.

[17] 李晖,孙文海,李凤华,王博洋.公共云存储服务数据安全及隐私保护技术综述[J].计算机研究与发展,2014(07)：1397-1409.

[18] Dale Peskin ,Andrew Nachison. Emerging media reshape global society[J].Media Emerging,2006(3):4-6 .

[19] Putnam ,Laurie L.Making Use of the Internet to Manage Emergency Services Information[D].San Jose State University,Pro Quest Dissertations Publishing,2003.

[20] Alexandra J.Campbell Relationship marketing in consumer markets [J].Journal of Direct Marketing,1997,11(3):44-57.

[21] 郭世斌,刘慧.美国、欧盟个人信息保护立法改革路径与启示[J].华北金融,2017(04):60-62.

[22] Christopher Kuner《European Data Protection Law》,Oxford :Oxford University Press,2007.

[23] Swire P P. 1997.Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information,in Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce. Ssrn Electronic Journal, 3(1):1-14.

[24] [美]尼格罗庞蒂.数字化生存[M].胡泳.海口：海南出版社,1996.

[25] [美]林德尔·G 霍尔库姆．公共经济学——政府在国家经济中的作用[M].北京：中国人民大学出版社,2012.

[26] [美]安东尼·唐斯.民主的经济理论[M].上海:上海人民出版社,2005.

[27] Kruger.H.A and Kearney.W.D.A Prototype for Assessing Information Security Awareness[J].Computers &Security, 2006(25):289 -296.

[28] Colin Tankard. Big data security [J]. Feature, 2012(7): 5-8.

[29] 丹尼尔·沙勒夫.隐私不保的年代[M].江苏:江苏人民出版社,2011.

[30] 周汉华.中华人民共和国个人信息保护法(专家建议稿) 及立法研究报告[M].北京: 法律出版社,2006.

[31] 郎庆斌,孙毅,杨莉.个人信息保护概论[M].北京:人民出版社,2008.

[32] 齐爱民.拯救信息社会中的人格——个人信息保护法总论[M].北京:北京大学出版社,2009.

[33] 胡皓渊.从网络个人信息资料看网络隐私权保护[D].上海:华东政法大学,2007.

[34] 《信息安全技术公共及商用服务信息系统个人信息保护指南》，工业和信息化部，2013年2月1日起实施，第一条规定：“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”。

[35] 奚晓明.最高人民法院利用网络侵害人身权益司法解释理解与适用[M].北京：人民法院出版社,2014:175.

[36] 王洋.基于网络安全的政府监管分析[J].中国市场,2016,(5).

[37] 胡敏洁,刘雪.网络发展与隐私权的保护[J]. 情报科学, 2002, 20(5):509-512.

[38] 李欲晓.云计算大数据时代个人隐私保护刻不容缓[J].理论导报, 2013(7):10.

[39] 张苇杭：“大数据时代我们需要个人信息保护吗?http://baijiahao.baidu.com/s?id=1584024651911593186&wfr=spider&for=pc.

[40] 张平.大数据时代个人信息保护的立法选择[J].北京大学学报,2017(03):147.

[41] 陈红.个人信息保护的法律问题研究[J].浙江学刊,2008(03):147-150.

[42] 王丽萍,步雷.信息时代隐私权保护研究[M].山东:山东人民出版社,2008.

[43] 李德成.网络隐私权保护制度初论[M].北京:中国方正出版社,2001.

[44] 秦尘.大互联网时代的隐私保护[J].软件工程师.2012(05):159.

[45] 熊进光.网络时代与隐私权的法律保护[J].江西社会学,2000(10)：132-135.

[46] 张继红.大数据时代个人信息保护行业自律的困境与出路[J].财经法学,2018 (06):58.

[47] 卢小宾,袁文秀.网络个人数据隐私权保护体系的三维透视[J].情报资料工作,2015(3):8.

[48] 王丽萍,田尧.论网络隐私权的行业自律保护[J].山东社会科学,2015(4):5.

[49] 蔡文通.网络时代个人信息保护问题研究[J].无线互联科技,2015(15):235.

[50] 王慧军.我国网络管理存在的问题及其改善[J].江西社会科学,2012,32(05):210-213.

[51] 舒筠云.非法获取公民个人信息罪的定罪问题研究[D].黑龙江:黑龙江大学.2014.

[52] 肖成俊,许玉镇.大数据时代个人信息泄露及其多中心治理[J].内蒙古社会科学(汉文版) , 2017(03):185-192.

[53] 工业和信息化部电信研究院.移动互联网白皮书[M].北京:工业和信息化部电信研究院，2014.

[54] 白雪.大数据时代的个人隐私如何保护[J].中国青年报,2014-09-25(02).

[55] 中华人民共和国工业和信息化部.《电信和互联网用户个人信息保护规定》.2013 年.第四条.

[56] 罗力.我国移动互联网用户个人信息安全风险和治理研究[J].图书馆学研究,2016(13):37-41.

[57] 刘筱娟.大数据监管的政府责任——以隐私权保护为中心[J].中国行政理.2017(07):56-60.

[58] 肖兴志,宋晶．政府监管理论与政策[M].大连:东北财经大学出版,2006:22-24.

[59] 刘鹏.西方监管理论：文献综述和理论清理[J].中国行政管理.2009(09):11-15.

[60] 孙毅,郎庆斌,杨莉.个人信息安全[M].东北:东北财经大学出版社,2012.

[61] 中宣部、信息产业部、国务院新闻办、教育部、文化部、卫生部、公安部、国家安全部、商务部、国家广播电影电视总局、新闻出版总署、国家保密局、国家工商行政管理总局、国家食品药品监督管理局等 2006 年印发《互联网站管理协调工作方案》通知.

[62] 国务院办公厅关于印发《工业和信息化部主要职责内设机构和人员编制规定》的通知国办发[2008]72 号.

[63] 《中国互联网协会章程》第二章第 6 条第 2 项规定：“制订并实施互联网行业规范和

自律公约，协调会员之间的关系，促进会员之间的沟通与协作，充分发挥行业自律作用，维护国家信息安全，维护行业整体利益和用户权益。”

[64] 《互联网信息服务管理办法》第 4 条：“国家对经营性互联网信息服务实行许可制度；对非经营性互联网信息服务实行备案制度……”

[65] 中国青年政治学院互联网法治研究中心.封面智库.《中国个人信息安全和隐私保护报告2016[EB/OL].https://mp.weixin.qq.com/s?src=3&timestamp=1576307939&ver=1&signature=zuLHuFwi-OxMLfjexcDn0gUw7RbEarFs*ynXMMO5ZOOoxVhy7j*Yz3EDYivAgiz7e2vUeYrxIrJKFA6-WOqjdaD7RAwkCch7w18q8pJdsjnywCe0ikklU5FeUQ1mccEjbdWwKck6NwyML7Ov0TbKVnotTH-FujFAE83N8vmS2rw=.

[66] 王艳.浅议信息化系统网络安全及防御措施[J].信息系统工程,2016(01):80.

[67] 徐闽斌,田勇,王书程.大数据安全问题的几点思考[J].信息安全与技术,2014,5(12):6-7+19.

[68] 胡利泉.谁掌握了“信息”就掌握了“未来”——我与《工会信息》30 年的渊源[J].工会信息,2018(12):17-18.

[69] 蔡长青.人民法院彻底告别人工统计时代[N].法制日报,2017-3-7.

[70] 陈美.国家信息安全协同治理:美国的经验与启示[J].情报杂志,2014,(02).

[71] 齐爱民.个人信息保护法研究[J].河北法学,2008(04)

[72] Jonathan P. Cody, Protecting Privacy Over the Internet: Has the Time Come To Abandon Self-Regulation? 48 Cath. U. L. Rev. 1183(Summer 1999).

[73] 宇贺克也,藤原静雄,藤井昭夫.回顾个人信息保护法立法过程[J].法学家,2003(12).

[74] 王融,石月.国际个人信息保护立法的新趋势与启示[J].电信研究院,2013(6).

[75] 齐爱民.拯救信息社会中的人格[M].北京:北京大学出版社,2009:290.

作者简历

一、基本情况：

姓名：王翠莹 性别：女 民族：汉 出生年月日：1995-05-05 籍贯：山东省潍坊市

2013-09——2017-06 聊城大学学士

2017-09——2020-06 中国矿业大学公共管理学院硕士

二、获奖情况：

2017.11 中国矿业大学硕士研究生二等学业奖学金

2018.11 中国矿业大学硕士研究生三等学业奖学金

2019.11 中国矿业大学硕士研究生三等学业奖学金

学位论文原创性声明

本人郑重声明：所呈交的学位论文《 移动互联网个人信息泄露政府监管研究》，是本人在导师指导下，在中国矿业大学攻读学位期间进行的研究工作所取得的成果。据我所知，除文中已经标明引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写过的研究成果。对本文的研究做出贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律结果由本人承担。

学位论文作者签名：

年　月　日

学位论文数据集

关键词*	密级*	中图分类号*	UDC	论文资助
个人信息泄露；政府监管	公开			

学位授予单位名称*	学位授予单位代码*	学位类别*	学位级别*
中国矿业大学	10290	管理学	硕士

论文题名*	并列题名*	论文语种*
移动互联网个人信息泄露政府监管研究	Research on Government Regulation of Mobile Internet Personal Information Disclosure	中文

作者姓名*	王翠莹	学号*	TS17090085A3MP
培养单位名称*	培养单位代码*	培养单位地址	邮编
中国矿业大学	10290	江苏省徐州市	221008
学科专业*	研究方向*	学制*	学位授予年*
公共管理	公共安全	三年	2020

论文提交日期*	2020 年 6 月

导师姓名*	曹明	职称*	副教授

评阅人	答辩委员会主席*	答辩委员会成员
	祝天智	王义保、许超、曹明、张彦华

电子版论文提交格式　文本（　）　图像（　）　视频（　）　音频（　）　多媒体（　）　其他（　）

推荐格式：application/msword; application/pdf

电子版论文出版（发布）者	电子版论文出版（发布）地	权限声明

论文总页数*	79

注：共 33 项，其中带*为必填数据，共 22 项。