内部资料·供领导/专家参考

城市发展动态

Urban Development Perspectives

2016 年第 9 期（总第 19 期）

华东师范大学城市发展研究院　　**2016 年 10 月 5 日**

信息化背景下城市安全问题探索

本期要目：

信息技术是城市安全的双刃剑

2016 中国电信诈骗形势分析报告

构建与时俱进的社会安全评价体系

物联网将带来新的网络安全问题

为维护城市公共安全注入“创新”力量

智慧城市环境下个人信息安全问题分析及立法建议

本期导读

信息科技为我们的城市安全提供技术保障的同时，也给我们的安全埋下了隐患。近日再次登上舆论的风口浪尖的电信诈骗案为我们敲响了警钟。如何在科技迅猛发展的当下，提前评测及预防危机事件的发生应当成为城市建设的重要议题。因此，本期《城市发展动态》聚焦于电信诈骗这一典型信息安全问题的现实风险及其相应对策，并结合境外经验措施以及相关领域的专家观点，为推进城市社会的信息安全提供参考。

领导批示	
专家反馈	

如有相关信息，请及时与本刊联系。（联系方式见封底）

目 录

一、本期热点：信息技术是城市安全的双刃剑 1

（一）信息化技术解决城市安全问题 1

（二）信息化技术带来城市安全问题 5

二、专题聚焦：积极应对信息安全风险 8

（一）2016 中国电信诈骗形势分析报告 8

（二）信息化时代的法制亟待完善 12

（三）构建与时俱进的社会安全评价体系 15

三、国际（境外）经验借鉴 18

（一）各国不同的诈骗手段 18

（二）实名与隐私的平衡 19

（三）警方和通讯运营商的做法 20

（四）安全意识的提升与严苛法律的震慑 21

四、专家观点 24

ROLF H. WEBER, EVELYNE STUDER：物联网将带来新的网络安全问题 24

M. BARTNES，N.B. MOE，P.E. HEEGAARD：系统学习能有效提升企业应对信息安全事件能力 26

柴俊勇：为维护城市公共安全注入“创新”力量 27

江时学：中国与欧盟在网络安全领域的合作探讨 28

曹树金等：智慧城市环境下个人信息安全问题分析及立法建议 29

一、本期热点：信息技术是城市安全的双刃剑

进入 21 世纪后，信息已然成为了第一生产要素，同时构成了信息化社会的重要技术物质基础。如今，各国大建信息高速公路，电脑广泛普及，这就给形成全球性的信息库和信息交换中心奠定了可靠和重要的技术物质基础。与此同时，伴随着城市化的脚步，作为以公众的健康、生命和财产免遭损害为目的，以法制化和社会化的防控方式，把各种威胁始终控制在某种最低限度，并尽可能保持公共生活的正常秩序的城市安全也已占据了城市治理的重中之重位置。在当今的上海，人口、功能和规模急剧扩张和复杂，而运行和管理更趋开放和自由，信息化时代下的城市安全面临着特殊的挑战。

（一）信息化技术解决城市安全问题

现代的特大城市，政府越来越关注城市集群的安全问题。城市周边地区和人口的持续增长，导致安全管理和安全保证更为复杂。与安全有关的活动牵涉到不同的实体：执法人员、服务提供商和基础设施运营商等。当城市出现安全问题时，必须对各方进行协调，以便有效地运作，此时就必须依靠信息通讯技术。因此，信息通讯技术在管理城市安全方面能起到至关重要的作用。

城市建设和信息通讯技术发展两者相辅相成。一方面，特大城市的持续扩张，为城市信息化和信息产业的发展提供了特别有利的环境；另一方面，依靠信息通讯技术管理城市，可以取得更好效果。

大城市需要有效的和可靠的监控和周边控制系统，以解决城市安全问题，包括高度集成的、地理上分散的视频监测、访问控制和防入

侵系统等，这也充分说明了信息通讯技术对城市安全的重要性。这些都是信息通讯技术为安全城市做出贡献的一部分。还有很多其他的城市安全解决方案，例如智能运输系统、智能电网和多式联运物流一体化系统等，这些系统都能纳入到安全城市平台，以便进一步创建“智能城市”，最终目标是关注市民日常生活的相关领域，明显提高人民的生活水平。

上海市在城市“网格化”管理领域一直走在全国前列。早在 20 世纪 90 年代就建立了网格化的预防体系，取得了良好的效果。2003 年以来,上海市积极响应党中央的号召,各区在社区网格化管理设想的基础上相继做了一些有意义的尝试。2003 年,《上海建设系统信息化规划纲要（2003-2010)》明确提出:“到 2010 年，基本实现城市管理对象的数字化、城市管理过程的数字化、城市管理评价的数字化，形成城市管理数字化的格局。”2004 年，上海市探索社区网格化管理的实践主要是围绕完善“两级政府、三级管理、四级网络”为特征的城市管理体制的新模式而展开。其主要内容包括：将街道(镇)划分成若干社区,以之为平台,理顺各方关系、整合行政职能、优化资源配置,形成资源统筹、职责明确、灵活反应、综合协调的网格化社区治理新模式,从而推动社区实体化。2005 年 7 月，建设部出台《关于推广北京东城区数字化城市管理模式的意见》，决定在全国推广数字化城市管理,上海成为首批试点城市。上海市建委借鉴北京市东城区的经验，发展了具有上海特色的城市网格化管理模式。市级工程投资 5678 万元，7 月开工，10 月系统开通试运行，并首先在长宁和卢湾两区开展试点，长宁区城市网格化管理系统同期投入试运营。从总体上看，上海城市网格化管理以信息技术为核心，以网格单元为基础，建立了指

挥、监督两大体系,通过网格化管理信息平台,推动问题的及时发现、快速处理和有效解决,实现了市、区、专业部门和监督员的四级联动、信息共享与资源整合。实现了管理对象数字化、信息处理网络化、市/区权责清晰化、工作流程规范化，使得城市管理水平得到了极大的提升。2006 年起，上海在中心城区全面推开城市网格化管理，将市政、交通、水务、房地、市容环卫、绿化等部门各自建立的 GIS 系统纳入网格化管理大系统中。浦东、徐汇、黄浦、静安等 4 个区在 2006 年 6 月开始试运行之后，市容面貌进一步改观,基础设施完好率明显提高。2006 年下半年,普陀、虹口、杨浦、闸北等 4 个区完成网格化管理信息系统建设；同时，还要启动松江、青浦等郊区城市化地区网格化管理平台的试点建设。2008 年至 2013 年，上海市网格化管理已经取得了丰硕的成果。已经形成了市、区、街道三级之间的大型数据库。市 1（市级平台）+17（区级平台）城市网格化管理平台全部建成，覆盖 200 个街道镇，共约 1200 平方公里主要城市化区域，涵盖 88 种类的部件和 32 种类的事件。目前，该系统已经集成公用设施、市容环卫、道路交通等 1134 万个部件信息，并实现了各个层面之间的实时沟通和信息共享。

近几年来，为推动和规范城市网格化管理工作，上海市政府陆续出台了《上海市城市网格化管理实施暂行办法》等规范性文件。同时《上海市城市网格化管理规范》、《上海市城市网格化管理考核评价办法》等一系列管理制度、标准和规范也相继出台。2013 年 7 月 29 日，上海市政府第 18 次常务会议审议通过了《上海市城市网格化管理办法》。在总结以往经验的基础上，完善了既有的概念、体制、规范、流程、标准等，明确了网格化管理机构的法律地位，以政府规章的形

式将城市网格化管理纳入法制化轨道，进一步强化了上海市城市网格化管理的功能与力度，形成长效机制。2014 年，为进一步整合各类城市管理资源，加强城市管理各相关部门的联动联勤，不断提升城市管理精细化、常态化水平，上海市人民政府印发了《关于深化拓展城市网格化管理积极探索和推进城市综合管理的若干意见》。《意见》明确提出，用五年时间，基本建成以城市网格化管理信息系统为核心，与“12345”市民服务热线相衔接，与“12319”城建服务热线相融合，并与其他相关行业管理信息系统互联互通的城市综合管理信息平台；基本建成市、区县、街镇三级管理体系，完善健全标准明确、管理规范、联动高效的城市综合管理监督指挥体系，形成与联勤联动工作机制的有效对接，实现非紧急类城市综合管理领域的全覆盖，全面提升城市管理水平。2014 年上海市委一号课题成果《关于进一步创新社会治理加强基层建设的意见》对于城市网格化管理提出了更高的要求，明确指出要“明确职能理顺机制，依靠‘网格化’去除城市管理顽症”。

从上海城市网格化管理的实例中，我们看到了信息技术参与城市治理过程中所取得卓越成果。在未来信息化进一步服务城市安全的过程中，要积极深入拓展和优化公共服务，凡属政府权责清单内的办事项，都要真正站在方便群众的立场上，逐步梳理纳入信息平台运行，实现流程再造，努力提供全方位、全覆盖、优质高效的公共服务。要以信息化技术为支撑，深化拓展网格化管理，加强网格员职能整合，推进网格员队伍建设，不断提升社会治理精细化水平，保障城市安全和百姓安宁。要进一步整合资源，将公共服务信息系统与视频监控系统建设融为一体，实现互联互通，加强安全保障，更好地发挥整体效益，确保城市安全，提升公共服务品质。

（二）信息化技术带来城市安全问题

在信息化背景下，探索城市安全的建设道路上，我们尚未积累丰富的安全运行和管理的经验。伴随其后续发展，公共网络在可靠性、安全性和响应及时性等方面，必然会造成城市管理上的脆弱性，并极有可能引发更为深刻的社会问题。

现阶段，我国城市中信息化技术面临的安全问题主要表现为以下几点：

1.他国主导核心技术。目前，许多核心技术仍掌握在外国公司手里：美国网络通信企业在我国硬件设施领域，近乎垄断地位;再者，例如微软、IBM、Oracle 等公司，在智慧城市的业务信息系统、数据库管理和业务解决方案市场，仍占主导地位。关键技术不在自己手中，日后很可能会存在一些不可控制的隐避信道和后门。

2.物联网技术安全问题。对于物联网技术的发展和应用，由于信息安全保障技术尚不成熟，可能存在许多安全问题，因设备不同，带来存储、处理及检测方式各异，使信息安全信息传送及处理亦较难统一；设备多数处于无人值守、自适应管理与自断、自通连接等状态，为安全系统的设计与实施增加难度。而这都需要一段时间的应用和发展才能慢慢完善起来。

3.终端安全问题。互联网环境下，难以保证所有终端设备都是安全的，而终端本身以及终端上的不安全应用，都有可能存在大量的安全问题。例如智能手机的操作系统将招致恶意软件的攻击;工控系统及智能移动设备，或成黑客攻击企业的主要途径，由此引起的数据销毁事件将会增多;通过手机僵尸等攻击手段，盗取手机中的数据，或利用手机定位设备跟踪手机用户。

4.尚未掌握的安全漏洞。云计算和通信基础设施可能存在我们尚未掌握的安全漏洞，云计算和通信基础设施一般由专业的服务提供商进行维护，这样可大大提升其安全性，但并不是绝对的安全，仍可能存在被人利用的安全漏洞。

5.自身存在的安全漏洞。城市生活中的各种应用不可避免地存在自身的安全漏洞，这与应用的设计和开发有关。换言之，经验和能力强的开发商提供的系统会更安全可靠。

6.安全防范管理，经验尚浅。作为一种新型的应用模式，较为传统的安全设备或系统，并不非常适用于现如今的应用环境，而适用的信息安全防护设备，又滞后于城市中信息科技的建设和需求，这势必会在一定程度上，造成安全防范管理上的漏洞。

随着物联网、云计算、大数据等高新技术的应用与发展，城市安全所要面临的网络环境更加复杂，使得信息、网络以及终端设备的安全更加严峻，而这些问题都要在建设过程中考虑全面，提前防范即将面临的安全威胁。我们面临的主要威胁集中在以下几点：

1.恶意网络攻击。未来的城市生活中提倡全面物联、透彻感知、深入智能化，能在任何时间、任何地点、利用任何设备登录网络，这让黑客更易于实施网络攻击，甚至进行“全面瓦解”。倘若成功攻破一个以二进制系统为基础的国家的安全漏洞，只需一个程序，便能掌握物联网应用的控制系统，从而控制目标地域的水、电、油、气、交通系统，随意瘫痪系统、夺取经济命脉、核弹解禁，试想如果成真将是多么恐怖的场景。

2.公共信息泄密。信息技术的各种应用是在公网上运行，收集并存储一个城市运行和管理的海量数据，海量数据经过数据软件分析后，

向城市管理人员提供该城市的各种重要信息，应对这些信息进行高密级保护。但由于这些信息设备多数处于无人值守的情况，攻击者可轻松盗取传感器件，获得存储密码和感知数据，通过多点放置被控节点副本及发射无线干扰信号等，从而进行物理层面攻击，最终使网络瘫痪;此外，还可利用公开的智慧城市应用和便捷的“云计算”资源，通过大数据计算，获取这些机密信息，一旦发生，轻则造成商业损失，重则将威胁到社会乃至国家的安全。

3.个人信息泄密。信息技术让生活中的各个方面进行互联，使得市民的个人信息在大量的网络应用上发布、原本在物理世界的生活却在网络上全面的留下足迹、个人和家庭的设施和物品通过物联网也暴露在了互联网上面。一旦个人信息遭到泄露，将对民众造成巨大的困扰和经济损失。由于个体经验的匮乏，加之没有安全防护的实践，导致人们普遍缺乏对个人信息的安全防范意识。

4.业务连续性和灾难恢复能力匮乏。伴随着信息技术的迅猛发展，人们的生活会越发离不开各种应用软件。很难想象如果出现应用的运行问题或者遭到自然灾害影响时，城市的运行和管理将遭受多大的创伤，必将极大的影响到市民的正常生活。

信息技术为人们提供了更智能、更互通的生活环境，但便利的网络环境以及个人信息的公开，势必会受到恶意攻击者的青睐。一旦灾害来临，将是一场不可估量的连锁反应，对此，我们更应提前做好充足的安全防护措施，去面对即将到来的信息安全威胁，将前车之鉴化作建设经验，降低不安全因素对社会、经济乃至国家安全的影响。

二、专题聚焦：积极应对信息安全风险

2016 年暑期，电信诈骗犯罪持续高发，给公众的财产和人身安全带来了巨大威胁。也因频发的案件带来的极为恶劣的社会影响，使得电信诈骗再次登上舆论风口浪尖，而在一次次的讨论抨击之后，在信息化快速发展的当下，各种不安全因素及各类诈骗案件几时能休，如何能休成为了当前亟待我们解决的问题。因此，本期专题聚焦首先从整体上对当前的电信诈骗问题进行分析，进而分析在信息安全问题中需要加强的诸如法制、社评体系的建设问题。

（一）2016 中国电信诈骗形势分析报告

9 月 7 日，中国最大的互联网安全公司 360 在京发布了《2016 中国电信诈骗形势分析报告》。这也是中国首份基于大数据研究的电信诈骗分析报告。360 互联网安全中心以 2016 年 8 月 360 手机卫士各项安全数据为基础，结合自身在安全领域的领先技术和丰富经验，对诈骗电话进行了深入的专题研究，深入了解诈骗电话的方式方法，并最终形成此份报告。报告从诈骗电话整体形势、诈骗电话类型、诈骗电话号源类型与归属、诈骗电话号源地域分析、电信诈骗攻击目标地域分析、诈骗电话攻击时间特点、电信诈骗识别力地域排行、电信诈骗典型案例拆解等角度，将当下猖獗的电信诈骗做了全方位解读。

仅 2016 年 8 月，360 手机卫士就为全国用户拦截各类骚扰电话 34.3 亿次，平均每天拦截骚扰电话约 1.11 亿次。其中，共拦截诈骗电话 4.45 亿次，占到了当月骚扰电话拦截总量的 13.0%，平均每天拦截诈骗电话约 1435 万次。考虑到诈骗电话可能给用户带来的经济损

失和其他严重后果，诈骗电话显然已经成为危害最为严重的骚扰电话类型。

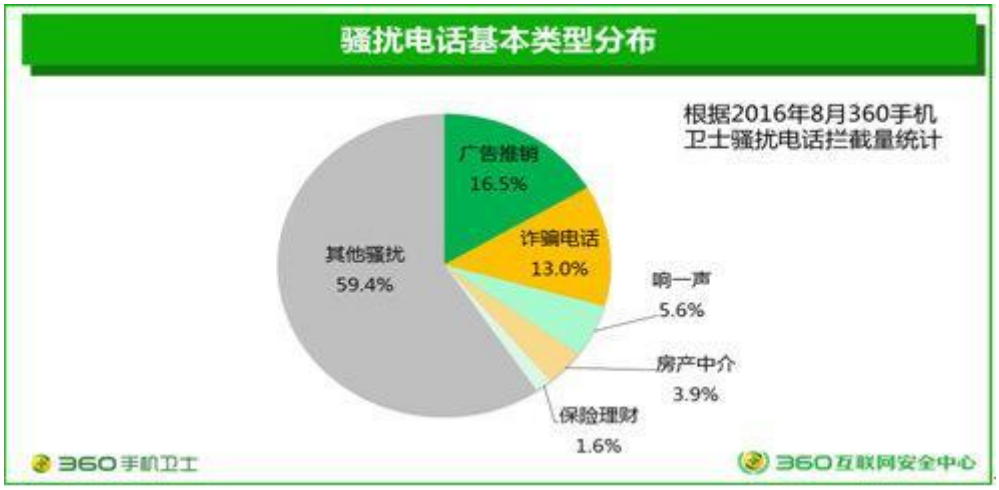

图 1 骚扰电话基本类型分布

“徐玉玉案”、“宋振宁案”、“清华大学老师被骗 1760 万案”……如今，电信诈骗受害人群已经覆盖了普通大学生、工薪阶层、高级知识分子等多个社会群体。同时，不法分子也有了一整套“成熟的方法论”，电信诈骗形成了一条从个人信息攫取、售卖到实施诈骗的黑色产业链，包括多个分工明晰的环节，十余“工种”环环相扣，将受害人一步步引入陷阱。对此，《2016 中国电信诈骗形势分析报告》做出了针对性极强的解读：

第一，金融理财类与身份冒充类诈骗占比近七成。根据 2016 年 8 月 360 手机卫士用户的“吐槽信息”的统计分析显示，在用户接到所有的诈骗电话中，虚假的金融理财诈骗最多，占 43.2%，此类诈骗在北上广深等大城市尤其盛行；其次是身份冒充诈骗，占 25.2%。两类诈骗相加占比 68.4%。在身份冒充类诈骗中，冒充电信运营商的诈骗数量最多，占比为 26.0%；其次是冒充领导，占 21.2%；排名第三的

是冒充快递，占 14.3%。

图 2 诈骗电话基本类型分布

第二，警惕不认识的固定电话和 400/800 电话。根据 2016 年 8 月 360 手机卫士拦截诈骗电话情况的抽样分析显示：在诈骗电话的号码源中，固定电话呼出的诈骗电话数量最多，占所有诈骗电话呼叫量的 56.0%；其次是 400/800 电话，占比为 27.1%；手机呼出的诈骗电话占诈骗电话呼叫总量的 15.4%；此外，还有 1.2%的诈骗电话来自境外呼入。可见，固定电话和 400/800 号码更应成为诈骗电话治理的重点对象。

图 3 诈骗电话号源基本类型分布

第三，骗子们的作息很规律。根据 2016 年 8 月 360 手机卫士拦截诈骗电话情况的抽样分析显示：每周五到下一周的周一，每天诈骗电话呼叫量均超过了一周总量的 15%，而周二到周四的呼叫量则相对较低。报告认为造成这种情况的主要原因在于，周末很多人都会独自在家，有空闲时间，而且身边没有可以给自己提醒的人，被骗子成功诈骗的几率也就更高。骗子们也因此选择在周末来拨打更多的诈骗电话。

不过从一天 24 小时的情况来看，骗子们的作息规律和普通人差不多。诈骗电话的高峰期出现在早上 8 点至 11 点，而晚上 10 点钟以后就相对较少，凌晨 1 点至 5 点是诈骗电话呼叫量的低谷期。

图 4 诈骗电话拨打时间一周七天分布

此外，根据用户举报及媒体报道，报告还对冒充公检法诈骗、冒充领导诈骗、冒充亲友诈骗、机票退改签诈骗、购物退款诈骗、假冒证券公司诈骗、利用无卡折业务退款诈骗、积金积存交易诈骗、邮政活期转定期诈骗等 9 类典型电信诈骗案例进行了解读与分析。

（参考资料：《360 发布电信诈骗形势分析报告▪金融理财诈骗超四成》，中国新闻网，http://www.chinanews.com/it/2016/09-07/7996902.shtml）

（二）信息化时代的法制亟待完善

舆论力量的推动和有关部门的全力处置大大加速了徐玉玉一案的破获，但不得不承认的是，不是每一个受骗的人都可以借力舆论，不是每一次被骗的金额都足以立案定罪，也不是每一次诈骗破案都会得到社会如此高的关注。生命逝去的背后，是一个亟需多部门合力整治的“陈年旧疾”。避免类似徐玉玉悲剧重演，不仅需要加强公众的防范意识，监管机构更责无旁贷。

诈骗团伙“产业化”、“企业化”已成事实。上海市公安局刑侦总队二支队副支队长韦健介绍，每一起通讯信息诈骗中，产业链上下游往往附着至少五个专业团伙：专司策划骗术、拨打电话的直接诈骗团伙；盗卖个人信息团伙；收集办理非实名电话卡、银行卡卖给诈骗分子的团伙；在互联网上搭建诈骗网络平台并与传统通讯网对接及提供任意改号、群呼服务和线路维护的技术支撑团伙；专门负责替若干个诈骗窝点转取赃款的洗钱团伙。

与此同时，在信息化时代，个人信息在无意或有意中都或多或少被泄漏，**犯罪源头的监管问题严重。**一报考职称英语，各种“培训”、“包过”服务就来了；一生完孩子各种“基因检测”、“满月照”推销就来了；一办信用卡，各种基金、保险很快找上门……从日常接到的骚扰电话我们均可感受，目前教育、医疗、金融，是信息泄露最厉害的领域！也是涉及百姓最深的公共服务领域。一般来说，这些公共服务部门收集信息，都带有一定强制性，不管是办理银行卡、生病住院、生孩子、还是参加各种资格考试，不提供身份证这个最重要的个人隐私是不可能的。而一旦个人信息从这些领域泄露，公众对危害行为将毫无防备，后果也更严重。所以，两个犯罪“终端”，源头只有

一个，相对于打击骗子，加强公共部门信息监管、人员监管、业务方式监管，加重对非法提供个人信息者的量刑，堵住信息泄露这个源头，永远更重要。

实名制并不是解药。按照工信部要求，在2016年年内，实名率要在95%以上。到2017年6月30日，实名率达到100%。从今年年初开始，各大运营商也陆续通过各种方式通知用户进行实名制。据了解，目前多地运营商的实名率早已超过95%，对于100%实名的目标也在不断推进。目前，难点在于存量的未实名认证用户，就得需要用户自主申报。在这种情况下，各大运营商已经先后公告，在要求的时间内未进行实名制的将停止服务。早在去年9月，广东就已开始执行“停机令”，今年8月初，天津、贵州、吉林等地也开始停止未实名登记号码的通信服务。但这个过程需要时间。根据广东电信的统计数据，截至目前，广东电信用户实名登记率达到96.24%，已关停50多万未实名用户。对于何时能消除未实名的电话“黑卡”，广东电信相关负责人预计会在半年内实现。

对于移动电话用户实名制，有观点认为，手机号码实名制是清扫诈骗行为的灵丹妙药，所以运营商在应该不计成本彻底解决实名制问题。似乎只要电话实施实名制，就能一劳永逸挖掉电信诈骗这个毒瘤了。情况真是这样吗？答案是否定的。就以跨国电信诈骗为例，诈骗团伙可以通过改号软件“借道”国内实名制电话进行诈骗。广东省公安厅公布的统计数据显示，近年来，在广东，跨国电信诈骗造成的财产损失已占所有电信网络诈骗犯罪的40%以上。其中，大部分是通过境外改号软件打入，冒充境内公检法等机关进行诈骗的。

所以，将电信诈骗横行归咎于运营商推行实名制不利，这一观点

以偏概全并不可取。要根治电信诈骗，仅依靠运营商的力量远远不够，要知道，对于诈骗分子来说，真的想要骗人钱财，“实名制”哪能斩断贪婪的手？只有靠健全而严厉的法律。

首先，在“裸奔”的信息社会，**公民信息安全保护和监管工作必须启动问责机制。**今年上半年，全国共破获电信网络诈骗案件5.7万起，是去年同期的2.5倍；查处违法犯罪人员2.8万名，是去年同期的2.7倍，但在这些案件中可以发现，依然存在不法分子的“数据黑色交易”，也有数据维护者的监守自盗，如果任由携带个人特质的信息片段，随意被公开、买卖，那么受骗悲剧仍将继续发生。

其次，通信业主管部门、电信运营商和虚拟运营商须尽可能**从技术角度杜绝诈骗电话存在。**实名制落实不力、运营商态度不明、相关监管措施不力，电信诈骗的多发已让通信业走到了不得不理清头绪、查堵漏洞的关口。在已曝光的电信诈骗犯罪中，实名制这道“马奇诺防线”却常常被绕过，这也暴露出其技术上的薄弱。广东电信相关负责人解释，按照目前的国际电话准入规范，境外电话经过改号软件拨入境内，就算其改号后的号码与境内的某一号码一模一样，只要符合号码规范，就是规范的，国际端口局并不会对这类号码进行拦截。也就是说，即便是国内移动端全部实名制，也难堵所有的诈骗通道。因此，我们应该从不断提升监管技术的角度出发，防患于未然。

最后，**沉疴用猛药，治乱需重典。**对于外漏的公民个人信息，一旦流到非法市场，将会给当事人带来无法估量的严重后果。有关专家指出，据对以往判决的分析，侵犯公民个人信息犯罪的量刑在实操中过于宽松，已不适应日益猖獗的个人信息犯罪。目前根据我国刑法规定，诈骗公私财物价值三千元至一万元以上的，即构成诈骗罪，处三

年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。在徐玉玉一案中，虽然诈骗金额不足1万元，但最终导致徐玉玉心脏骤停死亡，造成了严重的后果，才对犯罪嫌疑人从严处理。此外，相关案件的立案、取证过程复杂，往往因各种因素并不能得到有效处置。

相关职能部门不仅要在类似重大舆情案件面前挥出重拳，更要在日常为老百姓、为城市安全构建一道安全可靠的防火墙，真正把每一个公民的生命财产安全乃至国家安全时刻放在心上。

（参考资料：《九问电信诈骗：抓到骗子就完了？究竟谁卖了信息》，2016年8月28日《21世纪经济报道》（综合版）；《徐玉玉父亲的愿望如何才能成真》，2016年8月28日《新华每日电讯》（第2版）。）

（三）构建与时俱进的社会安全评价体系

各类诈骗案件仅仅只是信息科技时代里带来的众多社会问题里的一小部分。据美国ABC7 News报道，2016年8月7日，旧金山一名男子Calvin Riley在公园玩《精灵宝可梦Go》(Pokemon Go)游戏时，被枪击身亡，年仅20岁。在台湾，这款游戏已经进入疯狂的境界，日前由于稀有妖怪聚集，台湾北投公园近来因游戏爆红，广大玩家不分昼夜涌入公园，除了住户头疼之外，目前已经造成交通瘫痪，不少的司机也在抱怨无法正常通过这一区域。往往路面上人潮涌动，每个人都在低头看手机，可怜的汽车驾驶员“进得来出不去”，只能望着人潮苦叹。网友看了也傻眼，称满眼都是人，由于玩家过多，目前在当地已经出动警察维持秩序。与此同时，游戏今年夏天问市后，英国

各地警局一个月内接获将近 300 多起报案。忙着四处“抓精灵”的玩家，成了歹徒眼中的“肥羊”。英国大曼彻斯特警察局和伦敦都会区警察局都传出有抢匪利用诱饵，让受害人分心，伺机抢走手机案件发生。此外，今年 7 月初，美国一辆特斯拉 MODEL S 在自动驾驶时发生车祸导致驾驶员死亡，这是目前自动驾驶技术应用以来第一起已知的导致死亡的车祸。在我们分析事故产生原因的同时，也有不少人们开始议论事故责任应该如何认定等等。

在信息科技迅猛发展的今日，科学技术进一步拉近了个体、群体之间，社会国家之间以及现实与虚拟之间的距离，不断为我们的生活带来便利的同时，也对我们的城市治理工作提出了更高的要求，除了在法制规范领域内亟待我们的完善优化，更需要我们有更多防患于未然的考虑，而不再只是一味地亡羊补牢。这就需要我们**构建一套专业、科学并与时俱进的社会影响评价体系。**

关于科技发展对社会各方面的影响早已有很多学者们从哲学、政治经济学、社会学等角度进行了定性的评述。但是如何建立具体的评价指标体系、评价模型和方法，以定性和定量相结合来综合评价则无甚涉及。这一想法灵感来源于目前体系较为完善的“环评”，即环境影响评价（Environmental Impact Assessment，EIA）。它是指对规划和建设项目实施后可能造成的环境影响进行分析、预测和评估，提出预防或者减轻不良环境影响的对策和措施，进行跟踪监测的方法与制度。通俗说就是分析项目建成投产后可能对环境产生的影响，并提出污染防治对策和措施。

据此，在现阶段，我们不妨根据科学学、社会学、统计学原理和信息科技发展对社会的作用机制，选择与其关系较密切的一组社会领

域，建立反映这种关系的评测指标体系。在相关分析的基础上经过专家咨询确定指标及其权重，并结合国内外相关经验，探索构建一套符合我国国情并与时俱进的具有科学性的信息科技社会影响评价体系。不仅对科技创新产品的生产、推广进行源头监管，并提前预判其可能带来的社会问题，在其大规模运用之前做到心中有数，将可能带来的不良影响降低到最小。与此同时，该系统还应该开发各类项目产品上马后的跟踪监测功能，使得政府能够实时监管，对于产生的问题能够及时做出合理反应，并对已经产生的问题做出有效的危机干预。

三、国际（境外）经验借鉴

近些年来，伴随着信息科技的发展，各类网络及电信诈骗已经成为各国社会“顽疾”。人人都是个人信息的生产者，却不清楚个人的信息数据是如何被储备、保护、使用，甚至转让或买卖。通过调查，我们发现，这一问题并不仅仅困扰着大陆居民，而是在全世界各地蔓延。在这一发展过程中，国际（境外）有一些值得我们学习和借鉴的经验教训。

（一）各国不同的诈骗手段

通过发短信和打电话行骗的较低级的电信诈骗在德国还是比较罕见的。电信诈骗使用的一般来说是带有黑客性质的互联网行骗手段，比如说通过各种电脑病毒来调取信息，然后利用网络上的各种安全漏洞，诱使人上当受骗。有时候还有一些中奖信息，或者通过编造有未支付的账单，不立即付款就被告上法庭之类的。

日本电信诈骗多发生在老人身上。因为老人的积蓄丰厚，而且辨识能力弱，诈骗者常常冒充其亲人、子女、警方或银行，利用“垫付支票”、“修改银行卡密码”、“涉嫌非法活动”等谎言，欺骗这些老人进行转账汇款。

在美国，平均每分钟就有 5 通诈骗电话。骗子最常用的伎俩就是冒充税务部门，利用美国人对纳税的重视进行诈骗。还有，免费旅游、免费礼物等中奖信息也很常见。骗子们在电话里语速一般都很快，就是为了让你反应不过来做出错误选择。

澳大利亚电话诈骗方式主要是提供免费旅游、谎称“中大奖”、

“政府退税”等，其中针对移民的电信诈骗也比较流行，诈骗犯冒充移民部门官员给持临时签证的移民打电话，谎称对方签证出现问题，需要缴纳相关费用，否则将被驱逐出境。

（二）实名与隐私的平衡

实施实名制的初衷是严打诈骗分子的，但在业内人士看来，有心诈骗的人除了可以买到有实名认证的卡外，更是可以通过用假证件弄到手机卡，实名制反而给普通大众造成了安全隐患，因为我们的手机号、姓名和身份信息都有可能被诈骗分子获取，更便于其精准诈骗。

目前在市场上存在着专门买卖身份证及与之配套手机卡信息的行为，一套信息售价高达数千元。而这些信息的出口之一就是电信诈骗分子，很多参与电信诈骗的手机号都是实名制，但这个实名信息未必就属于实际使用人。更是有媒体报道称，预计有成千上万的身份信息在“黑市”里流转。所以，即便是实行了手机实名制，诈骗分子仍是可以通过买到手机号进行诈骗。

所以，随着近年来个人信息泄露事件带给用户困扰和担忧，公众对于实名制是否会引发隐私泄露产生忧虑。有声音甚至质疑，这是否形成了对用户隐私权的一种好意“妨碍”？

以网络实名制为例。2005 年韩国将网络实名制以立法形式付诸实施。但却事与愿违，实名制打击犯罪效果有限，个人隐私却大规模泄露。随后在 2012 年，韩国宪法裁判所 8 名法官一致做出判决，称考虑到网民个人信息通过网络泄露的危险性增加等种种情况，将废除网络实名制。

在我国推进电信实名制的过程中，应该重视的是，实名信息泄露

可能性一直存在，要提前做到对于个人隐私信息的保护，而不能一味将注意力放在实名制能抵挡网络诈骗这一角度上。

（三）警方和通讯运营商的做法

目前国内以170、171开头的号段是主要服务平台的虚拟运营商，他们不自己建设通信网络，而是租用实体运营商的网络开展电信业务。相应监管工作上还有待进一步提高，成立专门的监管机构，从技术上加强对公民信息安全的保护也不失为一种办法。

德国建立了完备的个人信用网络，所有人在银行开户，签订手机、网络等合同时，都必须进行实名登记。工作人员会严格审核用户身份，并签订“信用合同”，报备到德国信用信息处理机构 Schufa。一旦有人被骗，就能轻松查出相关信息，为受害者追回钱款，并扣除诈骗方的信用评分。

在日本，警方与银行联动，对账户的异常交易进行监控，对 ATM 机单日及单次转账额度进行限制，禁止账户买卖，规定在柜台转账超过 15 万日元时必须出示身份证。日本还有一种“手机会话分析”软件，它收录了大量诈骗高频词汇，能结合接听者语调的变化判断是否为诈骗电话。一旦认定是诈骗电话，手机就会发出警报声，并在屏幕上做出提示。

此外，2015 年，日本警方共接到超过 20 万起电话诈骗报警的案例，其中，60%的受害者是 60 岁以上的老人。从 2013 年开始，日本消费厅便拨款超过 10 亿日元，帮助老人们在家庭电话上安装一个录音机，帮助他们防范不法分子。在日本西南部的佐贺辖区，电话诈骗很猖獗，去年一年就有超过 1200 位老人因电话诈骗而报警。佐贺地

方政府于今年初率先得到了 1000 万日元的拨款，为辖区内的所有老人家中的座机免费安装了电话录音机。 据悉，虽然这种电话录音机目前尚未在日本全国普及，但从效果来看，佐贺辖区境内今年的诈骗案例已经大大减少，日本消费厅日前表示，今后将把这种电话录音机在全国推广。

美国推出了“拒绝来电名单”（Do Not Call），人们可以自主选择是否接受电话推销的来电。AT&T、苹果、谷歌、Verizon 等美国通信业巨头联合成立“反自动呼叫电话打击行动组”，他们将开发出一种主叫号码 ID 识别技术，来屏蔽那些假号码拨出的电话。此外，美国的 VoIP 网络电话领域还有一个名为 Nomorobo 的呼叫屏蔽服务，可以封锁自动呼叫电话。

澳大利亚电话局向民众开放申请免费的“电话号码保护”服务来拒绝所有市场营销人员来电，还设立了专门的报案网站。澳大利亚警方采用批处理技术、数据深挖技术、特征构化技术和 MDT 软件等措施预防及打击电信诈骗。

（四）安全意识的提升与严苛法律的震慑

其实早些年台湾当地的电信诈骗行为泛滥，但经过几年的发展，当地居民危机防范意识增强，使得诈骗团伙在当地没有市场，所以，近年来，台湾诈骗团伙频频在大陆开展诈骗，主要就是因为大陆人民防范意识较弱。所以，我国预防电信诈骗，应加大对“弱势群体”的宣传力度，深入农村等教育程度较低地区，开展有针对性的宣传工作，帮助人们有效提高对于电信诈骗的防范意识。

电信运营商曾想封停涉嫌诈骗的号段，却遇到了无法可依的窘境。

在信息化时代，防范各类诈骗，政府应与时俱进，加强立法，严厉打击泄露、倒卖个人信息的违法行为，增加侵害个人信息安全的违法犯罪成本。对于涉及个人信息采集的医疗、电信、银行等行业，制定完备的强制性行业规范。

从国外的相关法律法规来看，国外在防范电信诈骗时，首先做的就是推行个人信息保护法，对电话用户以及电子邮件用户进行教育，增强公众的法制观念和自我保护意识，使得用户在甄别电信诈骗、垃圾短信上具有绝对的主动权。

以美国为例，美国治理电信诈骗主要依靠两部法律。分别是 1991 年通过的《电话消费者保护法》，另一部是 2003 年生效的《控制非自愿色情和推销侵扰法》。两部法律明确规定，不得向消费者发送与商业营销、产品推广、服务广告有关的垃圾短信。用户只能在两种情况下接受此类手机短信：一是明确表示同意接收；二是这些短信用于紧急情况。

此外，2003 年，美国联邦贸易委员会根据《电话消费者保护法》推出“不接受电话推销名单”服务，全美任何座机和手机用户都可在这项服务的专门网站上免费登记。任何人向使用这项服务的用户发送未经同意的推广短信，都属于非法行为。

为了打击不法分子，防止老人上当受骗，日本在 2007 年通过了《假冒账户存入受害者救济法》保护诈骗的受害者，授权银行对可疑账户进行冻结，并对受害人的债务减记、受骗金额返回等做出规定。

以新加坡为例，其去年通过了个人信息保护法案，禁止向个人发送市场推广类短信等垃圾信息，违法发送垃圾信息的机构或个人可能会被重罚 100 万新元，约合 514 万元人民币，每条最高 1 万新元，约

合人民币 5 万多元。同时，新加坡政府将成立个人信息保护署，负责处理这一法案的相关事宜。正是由于这些法律法规的存在，用户无法收到诈骗信息，从根本上杜绝了网络和电信诈骗的高发风险。

伴随着信息科技的迅猛发展，在未来的个人信息安全、城市公共安全等领域内，我们除了在安全意识提升、运营监管、立法执法等方面需要向发达国家及地区取长补短，据其经验以儆效尤外，在探索构建科技发展的社会影响评价系统的道路上，还应注重和国际（境外）的协同合作，共同布控防控，通过各国各地区政府、企业、行业协会和用户多方参与，寻求主体间最大化的共同利益。

（参考资料：《日本老人怎样防止电话诈骗》，2016 年 6 月 22 日《中老年时报》（第 4 版）；《以国家行为列电信黑名单》，2016 年 9 月 4 日《山东商报》；《严防电信诈骗，国外都是怎么做的？》，新华网社交网络中心，http://sike.news.cn/hot/qazt2016/QA_dianxin/index.html；王大为，温道军：《预防与打击两岸电信诈骗犯罪问题研究》，《中国人民公安大学学报（社会科学版）》，2012 年第 2 期。）

四、专家观点

当前我国将互联网作为信息化发展的核心，与工业、商业、金融等服务业的全面融合加速布局“互联网＋”。由于缺乏对大数据时代电信诈骗井喷式爆发的前瞻性考量，以及保护民众法益的制度构建的缺失使得社会再度陷入了防范与惩治电信诈骗犯罪的困境。电信诈骗犯罪呈现出的跨境化、跨国化特点也使得对其防范与惩治的国际合作和司法协助亟待提上议程。

Rolf H. Weber, Evelyne Studer：物联网将带来新的网络安全问题

伴随着科技的发展，对于日益增多的各类网络攻击，人们似乎早已习以为常了。受害者也已从个人和初创公司发展到了全球 500 强的企业们。世界各国的执法机构和政府，相继引起了警惕。2014 年被称为“数据泄露之年”[1]，2015 年被业内评论员称为“数据泄露 2.0 版之年”。[2]虽然这些标签可能是过于笼统，哗众取宠，但它描绘了当

[1] Tara Seals, *2014 So Far: The Year of the Data Breach* (August 2014), http://www.infosecurity-magazine.com/news/2014-the-year-of -the-data-breach/; Ponemon Institute Survey, 2014: A Year of Mega Breaches (January 2015), http://www.ponemon.org/blog/2014-a-year -of-mega-breaches; Chad Hemenway, *A look back at 2014: The year of the data breach* (January 2015), http://www.cyberrisknetwork.com/2015/01/01/look-back-2014-year-of-the-breach/.

[2] See Jay Johnson, *If 2014 Was The Year Of The Data Breach, Brace For More* (January 2015), http://www.forbes.com/sites/danielfisher/2015/01/02/if-2014-was-the-year-of-the-data-breach-brace-for-more/#495d5a6c6ac3; Chris Paoli, *2015 Security Review: Top Hacks, Breaches and Cyber Scams* (December 2015), https://rcpmag.com/articles/2015/12/01/top-security-hacks.aspx.

前更频繁、更复杂和更严重的网络攻击现状。此外，相关研究指出目前的网络攻击已逐步转向更具破坏性，以及更广泛的个体攻击。

许多城市的信息安全中的网络漏洞急剧上升。新技术和全球互联技术的增长，也使得我们的社会生活对信息技术的依赖逐年增长。与此同时，网络攻击的复杂性和进入的低壁垒，使得以商品化形式进入市场的网络犯罪比比皆是，几何倍数骤增。

物联网的出现也极大地改变了网络威胁的情境。物联网是新一代信息技术的重要组成部分，也是“信息化”时代的重要发展阶段。其英文名称是：“Internet of things（IoT）”。顾名思义，物联网就是物物相连的互联网。这有两层意思：其一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；其二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信，也就是物物相息。物联网通过智能感知、识别技术与普适计算等通信感知技术，广泛应用于网络的融合中，也因此被称为继计算机、互联网之后世界信息产业发展的第三次浪潮。物联网是互联网的应用拓展，与其说物联网是网络，不如说物联网是业务和应用。因此，应用创新是物联网发展的核心，以用户体验为核心的创新 2.0 是物联网发展的灵魂。

研究者通过调查发现，由于物联网生态系统的日益拥挤和动态互联网的发展给我们的网络安全带来更大的挑战。通过探讨在物联网背景下的互联网变化的法律网络安全环境，探寻另一种监管方式，即选择适用的国际规章以及其他办法，解决物联网所带来的安全问题。

（参考资料：Rolf H. Weber, Evelyne Studer: Cybersecurity in the Internet of Things: Legal aspects, *Computer Law & Security Review*, Available online 3 August 2016. ）

M. Bartnes，N.B. Moe，P.E. Heegaard：系统学习能有效提升企业应对信息安全事件能力

国际上目前最新的网络攻击和威胁报告显示，工业控制组织已然成为了强有吸引力的攻击目标。新出现的各种威胁要求我们建立一套应对未知事件行之有效的能力。这种能力受到组织、个体以及技术因等素的影响。通过对挪威电力公司长达两年半的实地调研（半结构式访谈、文献分析、参与观察、问卷调查等），研究者们发现了改进企业信息安全事件管理办法。

研究发现在企业中应对信息安全事故的培训被赋予了较低的优先级，并且不同级别类型的员工对事件培训和处理的观点不一致。与此同时，IT 人员和控制系统的工作人员对于信息安全的理解存在较大的差异。此外，跨职能团队的缺失使得事件发生后的响应过程不具备整体性。

据此，在未来的企业中，为了提高应对信息安全事故的能力，我们需要定期举办培训课程，及时做出系统的安全及各项评估工作，尤其是评估轻微事故并得以改进系统的潜力。从一种特殊的专门培训过渡发展到一套系统的培训方法，这不仅需要公司自身更需要整个社会对信息安全问题的重新认识和定位。研究结果显示，系统的学习能够极大地提高企业中应对信息安全事件能力。

（参考资料：Maria Bartnes, Nils Brede Moe, Poul E. Heegaard: The future of information security incident management training: A case study of electrical power companies, *Computers & Security*, No.61,2016, pp.32–45. ）

柴俊勇：为维护城市公共安全注入“创新”力量

近段时间以来，一些地方发生的洪涝灾害和安全生产事故，引起了公众的广泛关注。就城市发展而言，水、电、气、交通、通信等网络造就了现代生活的方式，同时也造成了安全问题的多元性多发性。面对各种挑战，我们的城市公共安全工作需要积极创新。思想观念创新，牢固确立以人为本的安全发展理念。过去我们说“生产安全”，如今则叫“安全生产”。这样的转变意味着安全不是保障而是前提，没有安全一切都等于零。安全不能只是写在纸面上、喊在口头上，更要装在脑子里。只有让管理者知道怎么做，让市民知道怎么防范，让社会每一个成员知道怎么参与及监督，才能营造更有安全感的城市。制度建设创新，建立一套可操作、易推广、能复制的规则。自 2003 年“非典”之后，我国开始关注公共安全相关领域的立法，但城市公共安全立法中仍存在很多空白。比如，缺少一部《城市公共安全法》，这是城市公共安全体系的重大基础性缺失。缺少了法律的规范和约束，一些事情就容易带有人为的随意性，一些给城市公共安全带来威胁的行为也得不到约束。公众教育创新，着力提升安全防范意识和自救互救能力。目前，我国民众对公共安全知识普遍缺乏了解，安全防范意识薄弱。同时，由于缺乏自我保护的技能，当面对危险时，难以采取正 确的措施保护自己和他人。因此，这就需要把公共安全教育纳入国民教育和精神文明建设体系，展开普及教育。一方面，应从学校教育做起，各级各类学校要开设安全教育课程。另一方面，应严格开展各类安全演练，在实战演练中普及安全知识，强化安全意识。同时，健全公共安全社会心理干预体系，积极引导社会舆论和公众情绪，切

实提升全社会的安全素养与防范能力。信息共享创新，以大数据提升危机预警管理水平。公共危机有多个发展阶段，其性质和量级大多取决于孕育潜伏期。利用大数据的挖掘、分析、预测和流程整合功能，对危机全流程进行动态管理，可有效解决“重治轻防”问题，增强前期预警能力，有效控制危机扩散，减少人民群众生命财产损失。同时，与城市公共安全相关的各个部门必须打破部门资源界限，利用“互联网+”思维实现应急管理的资源共享。

（参考资料：柴俊勇：《为维护城市公共安全注入“创新”的力量》，《解放日报》，2016 年 8 月 16 日第 10 版。）

江时学：中国与欧盟在网络安全领域的合作探讨

在世界各国的经济和社会发展进程中，互联网的重要性愈益突出。但是，相对于网络安全（Cyber Security）而言的网络不安全（Cyber Insecurity）已成为一个全球问题（Global Issue），危害性极大，由其导致的经济损失不计其数。因此，如何维系网络安全已成为全球治理的重要组成部分。

中欧在网络安全领域加强合作，既有利于发挥双方在全球治理中的积极作用，也有利于推动 2003 年建立的中欧全面战略伙伴关系，更有利于发挥互联网在各种经济和社会发展进程中的巨大作用。中欧双方都主张在网络安全领域开展国际合作。中国认为，各国应在平等互利的基础上，通过建立双边交流机制，开展多形式、多渠道、多层次的交流与合作，就互联网政策、互联网立法、互联网安全等问题交流观点、经验和做法，平等协商解决分歧。欧盟认为，网络犯罪是跨国界的，因此欧盟及其成员国应该在打击网络犯罪的过程中加强与国

际机构或其他国家加强合作。合作的领域包括执法、信息的交流和共享以及网络安全技术的研发。

中欧在网络安全领域加强合作的方式方法可以多种多样，其中最重要的是以下几种：强化政治互信，进一步发挥中欧网络工作小组的作用，完善信息交流机制，举办网络安全联合演习，探讨中欧共建海底光缆的可能性，加强技术交流，中国同时与欧盟委员会及其成员国合作，推动中国军方与欧盟成员国军方在网络安全领域的合作以及在制定国际规则的过程中加强合作。

（参考资料：江时学：《中国与欧盟在网络安全领域的合作探讨》，《国际论坛》，2016 年第 4 期。）

曹树金等：智慧城市环境下个人信息安全问题分析及立法建议

2010 年全球超过一半的人口居住在城市，到 2050 年将有四分之三的人口居住在城市。2014 年 8 月国家发改委《关于促进智慧城市健康发展的指导意见》中明确提出了中国智慧城市建设的主要目标，其中一个重要方面就是加强居民、企业和政府信息安全保护以及基础设施安全保护以实现网络安全长效化。

智慧城市中个人信息安全是智慧城市建设中必须解决的根本性问题，除了从技术角度加强对智慧城市中个人信息安全的保护之外，更重要的是需要从立法角度详细分析智慧城市中个人信息安全保护存在的问题，并提出一定的立法建议以加快我国个人信息安全保护的立法进程，为个人信息安全保护提供法律保障。智慧城市建设中不可忽视的一个方面是个人信息安全保护的问题。

法律保护手段的缺失和智慧城市建设进程的推进，其矛盾的进一步激发将使得个人信息泄露问题不断涌现，将成为阻碍“智慧城市”城市建设最为重要的原因。鉴于此，通过分析智慧城市的内涵、信息类型和信息环境特征，结合现有国内外个人信息安全法律保护现状，系统深入地分析了信息产生阶段个人信息非法采集、过度采集、信息关联、无法关闭智能设备出现的风险，信息传播阶段蓄意攻击、窃取出现的风险，信息存储阶段信息失控、权限越界、密码泄露出现的风险，信息使用阶段未授权使用、已授权但用作它途和非法出售或者非法转让、出售授权出现的风险；政府作为智慧城市建设的主导者、政策与法律法规的制定者和智慧服务的提供者，存在个人信息集体越境外流、数据中心运营权利过度集中、监管手段和监管行为缺失、内部人员无意或故意泄露的问题；智慧服务提供商则主要存在信息安全技术投入不够、信息安全管理水平不高、与用户缺乏可靠的第三方协议以及企业间个人信息互换或泄露给第三方的问题；用户及智慧服务提供商之外的第三方个人信息非法买卖形成的黑色产业链问题。在此基础上，提出了个人信息权利保护立法原则、政府公权力适度立法原则、智慧服务提供商责任原则和第三方限制交易原则，个人信息权利保护立法原则包括告知／透明原则、合法／合适原则、可控／自决原则、安全保密原则、可申诉原则、权利不可剥夺原则和可继承原则七项立法原则；政府公权力适度立法原则包括法无授权不可为原则、监控／监管责任原则、公共利益原则、敏感领域特殊保护原则四项立法原则；智慧服务提供商责任原则包括最低准入原则、责任明确原则、责任连带原则、未经许可不可转让原则、鼓励行业自律／第三方审查原则五项立法原则；第三方限制交易原则包括严厉打击原则、区别对待原则、

过错推定责任原则三项立法原则。真正实现个人信息安全的保护仍然需要各级政府部门的高度重视，集各学者之大成，并在现有个人信息安全泄露问题的基础之上尽快制定出台一项专门的个人信息安全保护法。

（参考资料：曹树金、王志红、古婷骅：《智慧城市环境下个人信息安全保护问题分析及立法建议》，《图书情报知识》，2015 年第 3 期。）

城市发展研究院·简介

华东师范大学城市发展研究院是为适应新时期学科建设、经济社会发展的需要，于 2013 年 10 月组建的跨学科、开放型、国际化的综合性实体研究机构。旨在遵循“政产学研用”一体化原则，创建学界、政界、商界融合互动的城市研究“学术共同体”，打造国内领先、国际有重要影响的城市科学研究基地，建设城市发展高端智库，成为富有活力、机制创新、资源汇聚、专家集萃的城市发展协同创新平台。原上海市副市长胡延照与华东师范大学校长陈群担任研究院理事长，原华东师范大学党委副书记罗国振担任副理事长。研究院首任院长为胡延照，现任院长为曾刚；张永岳担任副院长。

目前，研究院与国内外相关组织和机构展开深度合作，围绕上海全球城市发展战略、长三角城市群一体化、长江流域中国经济新支撑带建设等国家重大战略问题，开展联合攻关，以建设中国城市科学学派，为国家和上海及各地发展提供决策咨询服务。

特别声明

本刊是一本非商业、公益性内部参考材料，信息来源于互联网、公开出版物及专家投稿，相关观点不代表本刊立场。若对本刊作品内容、转载等事项有何意见和要求，请与本刊编辑部联系。

地址/Add：中国上海市中山北路3663号华东师范大学地理馆309室（200062）

Room309, Geography Building, East China Normal University

3663 North Zhongshan Rd., Shanghai, China (200062)

网址/Website： http://www.iud.ecnu.edu.cn

联系电话/Tel： 021-62232952

电子邮箱/Email: office@iud.ecnu.edu.cn

联络人/Contact: 罗峰LuoFeng