背景材料：

1.2016 年某工作日早上 7 点，北京某杂志社编辑叶女士出门上班，等电梯时，她在手机上点下“滴滴打车”软件的图标，之后，在小区门口的超时挑了一款面包，她把手机交给收银员用微信进行支付。走出超市，她预定的出租车正好到达。20 分钟后，用微信支付完车费，她像往常一样推开单位对面那家麦当劳的门—要了杯奶茶，找一个临窗的座位，掏出手机，WIFI 信号自动连接。

早上 8 点，叶女士坐在办公室前，打开电脑，她发现网页的右下角，居然跳出前一天自己在网上搜索的马桶水箱密封图片的窗口，而且网站同时提供了几种样式可对比。这一天，叶女士的手机收到 5 个呼入电话—你的房子要不要出售，有一份不错的理财要不要考虑，全英文精品班招生……现在手机铃响，不是广告就是推销，我很少用手机打电话，家人、朋友甚至包括领导、同事，真有事时都用微信沟通。”叶女士一脸无奈。

在互联网告诉发展的时代，大数据的综合运用为人们工作和生活带来便捷的同时，个人信息泄露，也影响到个人的生活、社会的稳定。

2.随着互联网的普及以及网络应用特别是网络交易的快速发展，消费者的个人信息也在以各种各样的形式在互联网上被采集、存储和传输。互联网在为消费者提供各种便利的同时，也为个人信息的泄漏提供了更快的传播方式和更多可能的传播途径。3 月 13 日，中国消费者协会公布的《2014 年度消费者个人信息网络安全状况报告》显示，利用网络“窃取”“非法使用”消费者个人信息的黑色产业链呈现出低成本、高技术、高回报的爆发性增长态势，并且已经从半公开化的纯攻击模式转化为敛财工具和商业竞争手段，集团化、产业化趋向明显。消费者因个人信息泄漏导致的经济损失数目惊人。

回顾一下前几年发生的重大网络安全事件:12306 铁路客户服务中心网站被黑客“撞库”，13 万条个人信息被泄露;支付宝前员工被曝贩卖 20G 用户资料;携程网出现安全漏洞，导致大量用户银行卡信息泄露;130 万考研考生报名信息泄漏，数据被多次转卖……据调查，约三分之二的受访者在过去的一年内个人信息曾被泄露或窃取。

当前消费者个人信息在网络安全方面面临两大风险点：第一风险点是网络服务商通过技术手段对消费者个人信息进行主动获取与海量存储。通过用户的主动提交、云服务的获取、网络服务商对用户行为的跟踪记录、手机应用软件等获取消费者的个人信息，或通过其他形式在消费者不知情的情况下获取消费者个人信息。这些信息因互联网服务商的不当管理，给消费者带来风险或造成损失；第二类风险点在于不法分子通过多种方式对消费者个人信息

的获取与非法应用。主要表现为:商家盗卖，一些掌握大量消费者个人信息的商业机构，因管理不善，导致内部员工盗卖消费者个人信息事件频发;网站数据窃取，一些存在高危漏洞的网站成了数据泄密的主要原因;木马钓鱼盗号，常常伪装成流行的应用软件或钓鱼网站套取消费者个人信息;二手手机泄密，通过恶意恢复消费者的二手手机数据，掌握大量消费者的个人信息;新型黑客技术窃取，利用伪基站以任意号码向消费者发送诈骗信息。

3.“我做网络反诈骗研究两年多了，每年都会受理 3 万多起用户投诉。有时候，当我们发现一些企业信息管理有漏洞时，多次找他们，但不知道为什么，有些企业就是不处理。我个人觉得，相对于经营者花大精力与技术力量对网络用户终端设备进行个人信息收集而言，他们在针对已掌握的消费者个人信息保护方面的投入明显不够。”某网络专家裴智勇说。

据业内人士透露，在一些行业里，消费者的个人信息常被当作个人谋取新职务或跳槽的见面礼。例如，保险行业的基层业务人员，他们掌握着大量客户的个人信息，包括健康信息、经济信息，个人账号，他们频繁跳槽，客户的信息就被一次次泄露。此外，房屋中介人员、教育机构的工作人员跳槽，也会导致个人信息泄露。

然而，与一个企业甚至一个行业的失范相比，个别员工的违规行为只能算作“小巫见大巫”。在今年央视 3·15 消费者维权晚会上，央视调查记者曝出，令人不堪其扰的骚扰电话，其幕后推手竟是电信运营商。这些电话，一天来电好几次甚至十几次，有时还冒充警方、银行等进行诈骗。据记者调查，骚扰电话之所以能大行其道，正是因为中国移动、中国铁通等电信运营商在为他们提供运营通道。

原本应该起到“防火墙”作用的服务商，却沦为不法分子违法犯罪的帮凶。这样的内幕令人震惊。“企业保护消费者个人信息的安全，既是法定义务，也是合同义务。如果企业失去了老百姓的信任，如果掌握海量消费者个人信息的企业不能保护消费者的信息安全，是一定会被消费者抛弃的。”中国工商银行消保办主任董建军介绍，多年来，工商银行从机制、技术和人员管控等多方面为保护消费者个人信息作出努力，目的就是确保客户信息不被泄露。

4.如今，外出就餐刷卡结账已成为很多人的一种习惯。“一些消费者付账时，经常会把卡直接给服务员去刷，这种任性行为，很可能会带来大麻烦。如果别人拿去复制一张，你的钱就会出问题了。所以刷卡时一定要记住卡不离身，消费不离视线。”中国银行业协会行业服务周总监说。

北京市消费者协会屈秘书长说。 “在今天这个时代背景下，消费者的权利保护意识亟

待加强。在日常生活中，无论是你的消费行为还是其他日常生活行为，都会留下一些痕迹，而这些痕迹在不经意间有可能就被他人恶意获取。比如，在一些大大小小的会议上，都会印发参会人员的通讯录。我多次发现，有些与会者离开的时候，认为那些会议资料没用了，就把它们丢在宾馆或会议室，一些重要信息就在不经意间流露出去。”

《2015 年度消费者个人信息网络安全状况报告》中关于消费者个人信息自我保护意识的调查显示，54%的受访者认为自己个人信息保护意识一般。具体表现为，在上网过程中，很多受访者都采取了个人信息保护措施，如安装安全软件，定期更新杀毒软件，不随便点击可疑链接，不轻易登记身份信息等，但采取“不同用途的账号设置不同的密码”、不轻易在公共场所连接 WIFI、不随便在移动设备充电站充电”等保护措施的受访者相对较少。

针对现在不少人热衷的海外代购，有关专家也提醒，对相关网址，一定要上网查询它是否在国内备案。此外，不要轻易把身份证扫描件给他人，扫描件一旦给了别人，意味着有可能你的一生别人都会拿着你的扫描件去进行非法操作。

绝大多数消费者对信息保护的法律法规了解较少或不了解。已实施的新消法在个人信息保护方面作出明确规定，经营者未经消费者同意或请求或消费者明确表示拒绝的，不得向其发送商业信息。而调查显示，46.64%的受访者在明确表示拒绝后，依然收到服务商发送的商业性信息。当受访者的个人信息被侵害后，超过 38%的人表示习以为常，选择保持沉默。

5.现在消费者个人信息受侵犯已成为社会公害，个人信息一旦提供出去，好像没有任何力量去保护已经提供的或被泄露的信息，那么，是不是只能任人宰割呢?”我们国家早就制定了相关法律保护个人信息。

2009 年刑法修正案(七)增加了“非法提供公民个人信息罪”和“非法获取公民个人信息罪”，即:“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金。窃取或者以其他方法非法获取上述信息，情节严重的，依照前款的规定处罚。”这一规定是我国首次从刑法高度对公民的个人信息予以保护，也弥补了刑法在打击侵害个人信息犯罪方面的空白，但该条文只对严重侵害公民个人信息的行为予以制裁，无法调整未达到情节严重标准的其他侵害行为。值得注意的是，司法实践表明，侵犯公民个人信息的主体范围已经不局限于国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，还包括其他主体，如实施侵犯公民个人信息的房产中介及互联网从业人员。

作答要求

根据给定资料，概括当前个人信息保护存在的主要问题。（20 分）

要求：概括准确、全面，条理清楚，字数不超过 300 字。

参考解析：

1.互联网为个人信息泄露提供了更快的传播方式和更多传播路径；利用网络窃取个人信息的产业链呈增长趋势、集团化、产业化明显。

2.互联网服务商不当管理，网络服务商为违法犯罪提供运营渠道；企业对个人信息保护投入不足，存在管理漏洞，处理不及时；企业员工为谋求新职务泄露个人信息。

3.不法分子通过多种方式对消费者信息进行获取与非法应用，包括木马病毒盗号、钓鱼网站、二手手机信息恶意恢复、新型黑客技术、伪基站等方式。

4.消费者权利保护意识一般，亟待加强，对信息保护的法律法规了解少。

5.法律机制不健全，无法调整未达到情节严重标准的侵害行为。

关注“天津华图”微信公众号：tjhuatu

后台回复“时政”可获取最新时政信息