

**软件法律法规与社会发展期末论文**

**论大数据时代下隐私泄露的伦理问题**

|  |  |
| --- | --- |
| 学 院： | 软件学院 |
| 专 业： | 软件工程 |
| 学生姓名： | 吴文韬 |
| 学 号： | 20373914 |
| 指导教师： | 赵精武 |

2023年12月1日

Catalog

**[一、 摘要及关键词 2](#_Toc1102120270)**

**[二、 引言 3](#_Toc1288922515)**

**[三、 案例简介 3](#_Toc1253162316)**

[（一） 中国电信超2亿条用户信息被卖 3](#_Toc1526918883)

[（二） 某英国安全公司云泄露50亿条安全记录 3](#_Toc496084931)

[（三） 锻炼跟踪应用程序Jefit数据泄露事件 4](#_Toc1167917663)

**[四、 大数据时代隐私泄露问题的提出 5](#_Toc1191628461)**

**[五、 大数据时代隐私泄露问题的相关调查 5](#_Toc267052105)**

[（一） 调查数据 6](#_Toc103906505)

[（二） 调查结果分析 12](#_Toc452424524)

**[六、 大数据时代隐私泄露问题的伦理保护难点 12](#_Toc1806864488)**

[（一） 大数据时代，个人权利和个人隐私保护存在天生的矛盾性 12](#_Toc405197589)

[（二） 互联网大公司的数据垄断严重影响了社会公平 13](#_Toc485233686)

**[七、 普通人应该如何应对大数据时代的隐私泄露 13](#_Toc1327152943)**

**[八、 总结 13](#_Toc1694355259)**

**[九、 参考文献 14](#_Toc1395678793)**

1. 摘要及关键词

大数据技术在给人们工作和生活带来巨大便利的同时，也产生了诸如个人隐私被泄露、数字身份遭盗用、数据安全受侵害、数字鸿沟（信息茧房）等越来越明显等一系列伦理问题。但是在大数据时代，我们在态度上反对泄露隐私，却无法拒绝技术带来的便利性。对此，有必要从大数据技术使用主体因素、大数据技术本身、大数据技术监管环境入手，分析其伦理问题产生的根源，并尝试进行有效治理。

摘要：大数据、个人隐私、伦理、市场监管

1. 引言

近年来，随着大数据基础设施建设（4G乃至5G的出现）的完善以及人工智能大模型技术的发展（GPT3.5乃至GPT4.0的问世），社会中不断涌现的新技术大大便利了人们的日常生活，但所谓“技术的价值在于它如何为人类社会带来更多便利和效益，而非仅仅停留在技术本身的发展”，智能化系统在服务人类生活的同时，其巨大的信息-经济利益也使得某部分人铤而走险，隐私数据泄露风险也愈发严重。当面对大数据时代的隐私泄露问题时，我们应该如何建立一个适配的规则，并能否借助该规则对我们的个人隐私信息进行保护，这值得我们进行深入的思考和研究。

1. 案例简介
2. 中国电信超2亿条用户信息被卖

2020年1月3日上午，中国裁判文书网公布了《陈德武、陈亚华、姜福乾等侵犯公民个人信息罪二审刑事裁定书》。

经法院二审审理查明：2013年至2016年9月27日，被告人陈亚华从号百信息服务有限公司（为中国电信股份有限公司的全资子公司）数据库获取区分不同行业、地区的手机号码信息提供给陈德武，被告人陈德武以人民币0.01元/条至0.2元/条不等的价格在网络上出售，获利金额累计达人民币2000余万元，涉及公民个人信息2亿余条。

1. 某英国安全公司云泄露50亿条安全记录

据外媒报道，2020年3月，安全专家Bob Diachenko发现了一个疑似属于英国安全公司的一个不安全的Elasticsearch实例，其中包括在2012年到2019年之间和安全事件有关的50亿条记录。

根据Bob Diachenko的说法，在3月16日，他在公网发现了一个缺乏保护的Elasticsearch实例，根据SSL证书和反向DNS记录，发现这个Elasticsearch似乎是由一家英国安全公司所管理。而且特别讽刺的是，其中包括一个“数据泄露数据库”，收集了2012年至2019年期间大量被报道（或许还有未报道）的安全事件中的数据。

这个巨大的Elasticsearch由两个集合组成，一个包含了5,088,635,374条记录，另一个正实时更新，包含1500万条记录。被泄露的数据包括：哈希类型（显示密码的方式：MD5/哈希/纯文本等）、泄漏日期（年）、密码（哈希值或纯文本）、电子邮件、电子邮件域、泄漏源（某些显眼的泄漏源：Adobe，Last.fm，Twitter，LinkedIn，Tumblr，VK等）。

1. 锻炼跟踪应用程序Jefit数据泄露事件

锻炼跟踪应用程序Jefit在2020年3月份发现了因安全漏洞而导致的数据泄密，这起事件影响了2020年9月20日之前注册的客户帐户。不法分子访问了以下信息：Jefit帐户用户名、与帐户关联的电子邮件地址、加密的密码以及创建帐户时的IP地址。Jefit保存IP地址用于防止机器人程序，并将滥用帐户登记在册。该公司查明了数据泄密的根本原因，并证实Jefit的其他系统未受影响。Jefit表示，它已采取安全措施来加强网络，以防范将来出现类似的泄密事件，并正在其产品上采用更加强大的密码策略，以便将来进一步保护用户帐户。此外，Jefit表示，敏感的财务数据未受到牵涉，因为该公司从不存储客户的付款信息。客户在Jefit网站购买产品时，所有支付流程都由Google Play Store 、 Apple App Store直接处理，或者由支付网关公司直接处理。

1. 大数据时代隐私泄露问题的提出

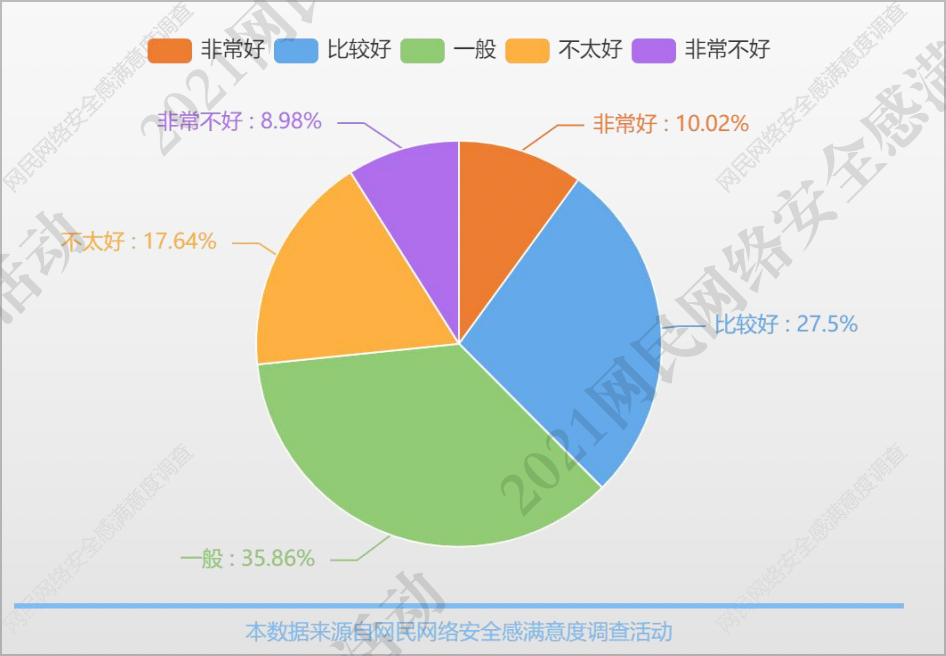
随着时代的变化，隐私的概念在不断的变化和扩大，并由于互联网信息的价值性以及各大公司算法对隐私数据需求的倾向性，个人隐私在大数据时代具有相当程度的直接价值。当我们在网络上进行注册、交易时，需提供各种私人信息，如姓名、电话号码、身份证号码、家庭住址等，这些信息很可能被非法分子恶意搜集利用甚至倒卖，导致个人隐私泄露。并且不法分子在盗取他人数字身份后，往往借用其身份从事犯罪活动，给受害者造成不可估量的经济、身份损失。

关于大数据时代隐私泄露问题的分析：1. 互联网范围的扩大，信息网络的全球覆盖、各大app无孔不入的数据收集、各式各样的监控摄像头等等无一不使网络的覆盖范围急剧变大，这也变向为不法分子攫取个人隐私提供了便利。2. 个人隐私的经济利益，所谓“无利不起早”，个人隐私数据作为一种信息资源，已经可以在市场上通过数字货币交易的形式来获取利益（比如暗网常见的UTC数据售卖），有需求就会有市场，这点无法回避。3. 隐私保护难度的提高，也是第一点导致的，大数据时代信息技术的发展远远突破了互联网早期的时间空间范畴，时间上，现如今的RAID阵列存储是的云数据故障的风险大大降低，这也导致了时间线回溯的可能性，空间上，各类摄像头的无死角覆盖也是的个人隐私保护形同虚设。

因此，个人认为如何提高隐私保护的技术手段和加强隐私保护的法律手段会是未来很长一段时间内的研究方向。

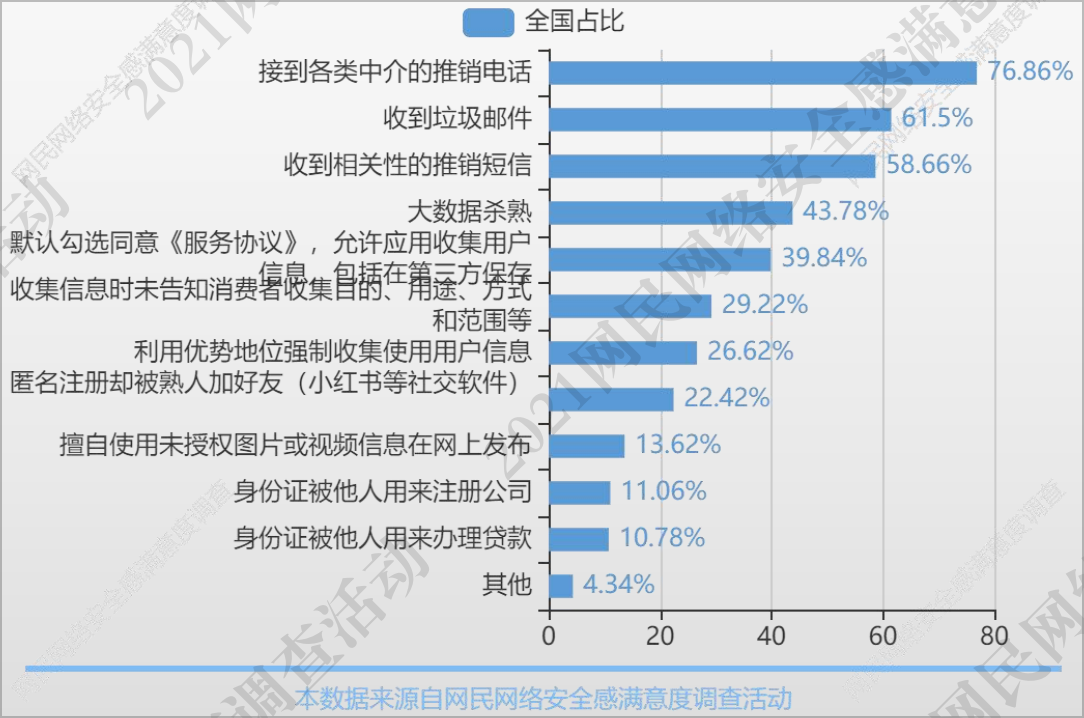
1. 大数据时代隐私泄露问题的相关调查
2. 调查数据
3. 公众网民对个人信息保护和数据安全的感受情况

根据数据显示，当前我国个人信息保护的现状呈现“三三分”态势：约37.52%的受访人群认为我国个人信息保护的状况“相对较好”，甚至是“非常好”；大约35.86%的受访人群觉得状况“一般”；还有大约26.62%的受访人群认为状况“不太理想”或者“非常不理想”。



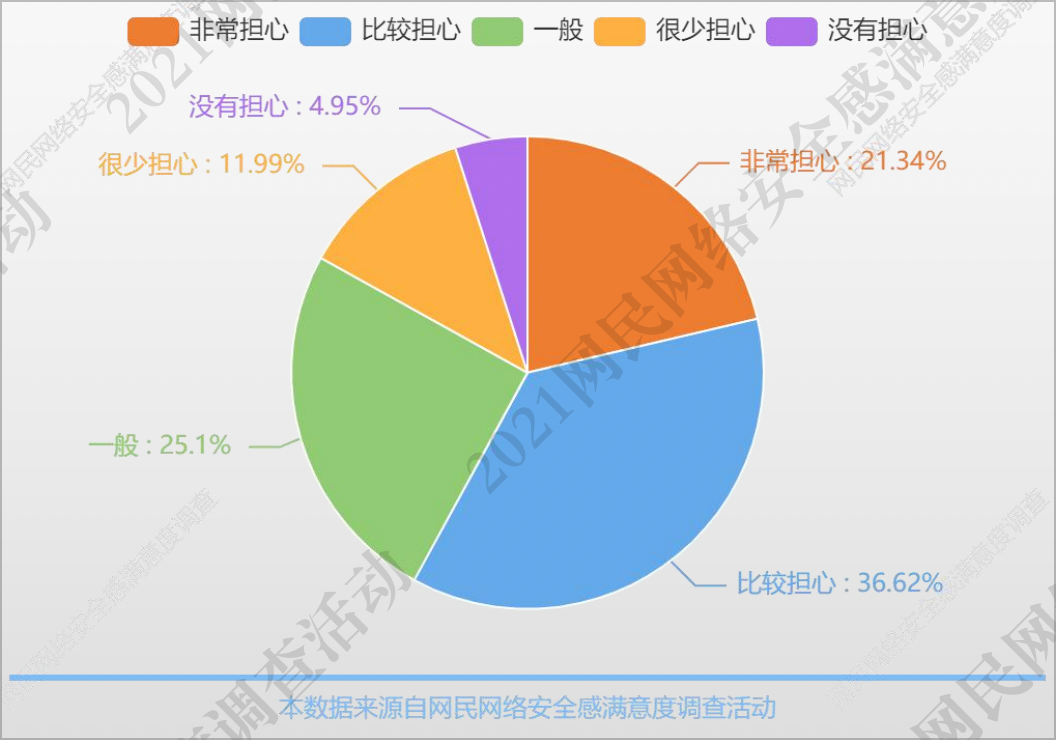
1. 公众网民对个人信息风险的感受状况

近八成网民接到各类中介的推销电话；超六成网民收到垃圾邮件；近六成网民收到相关性推销短信。除上述骚扰方式，公众网民还可以从其他途径推测出个人信息风险，例如超四成网民认为遭遇大数据杀熟是因为个人信息已泄露，近四成网民认为，默认勾选同意《服务协议》，允许应用收集用户信息，会导致个人信息泄露等等。



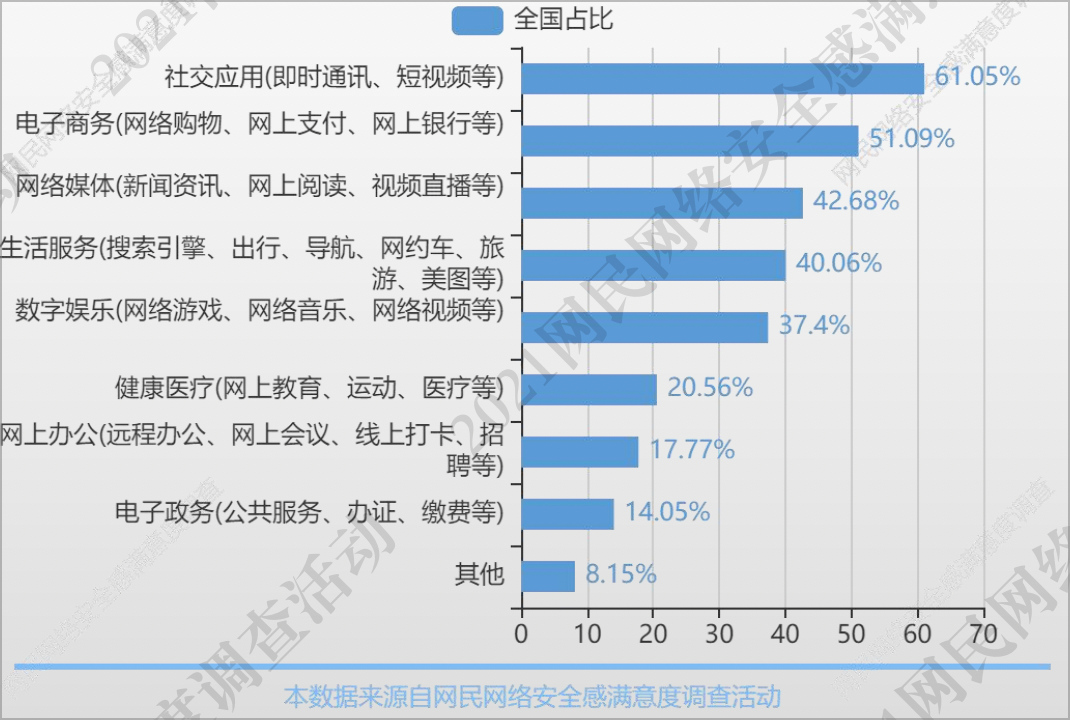
1. 公众网民对生物识别信息的风险感知

使用生物识别技术进行身份认证已成为社会生活的常态，但由于生活识别信息的不可更改特点，网民对生物识别信息的利用充满忧虑。57.96%的网民对生物识别技术的安全性“比较”或“非常”担心；25.1%的网民态度“一般”，无明显倾向；仅16.94%的网民对生物识别技术的安全性“很少”或“没有”担心。



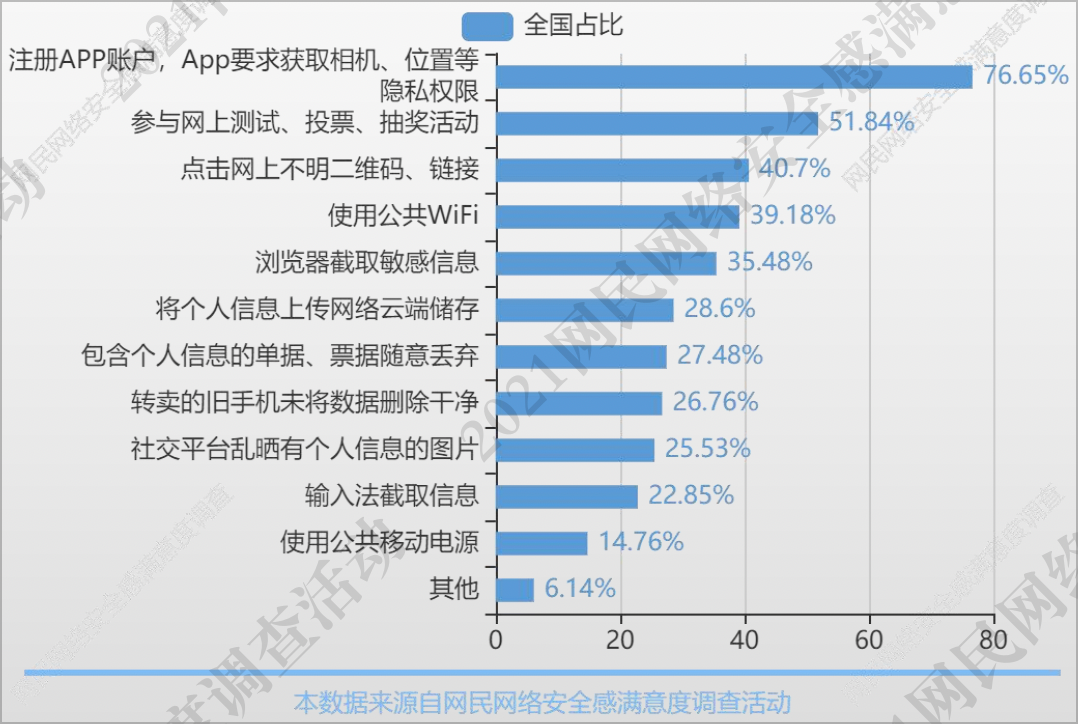
1. 公众网民对各类网络服务的个人信息风险感知程度

公众网民认为不同类型网络服务的个人信息风险不同，其中，社交应用类网络服务的个人信息风险最高，超过六成的网民认为其存在风险；网民认为电子商务类、网络媒体类、生活服务类和数字娱乐类网络服务存在较高程度的个人信息风险，而健康医疗类、网上办公类以及电子政务类网络服务的个人信息风险相对较低。



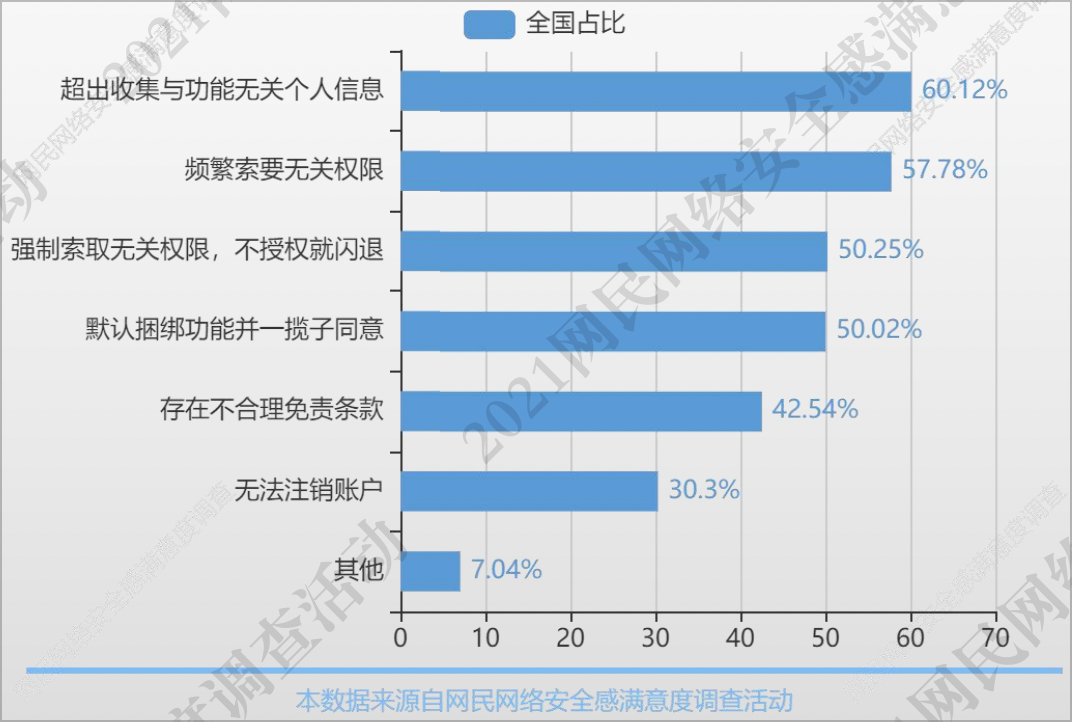
1. 公众网民认为个人信息泄露可能发生的环节

公众网民认为最可能泄露个人信息的途径是注册APP时，APP要求获取相机、位置等隐私权限，占比高达76.65%；其次，超过半数的受访群体认为参与网上测试、投票、抽奖活动可能会导致个人信息泄露；超过四成网民认为点击网上不明二维码、链接可能会泄露个人信息。



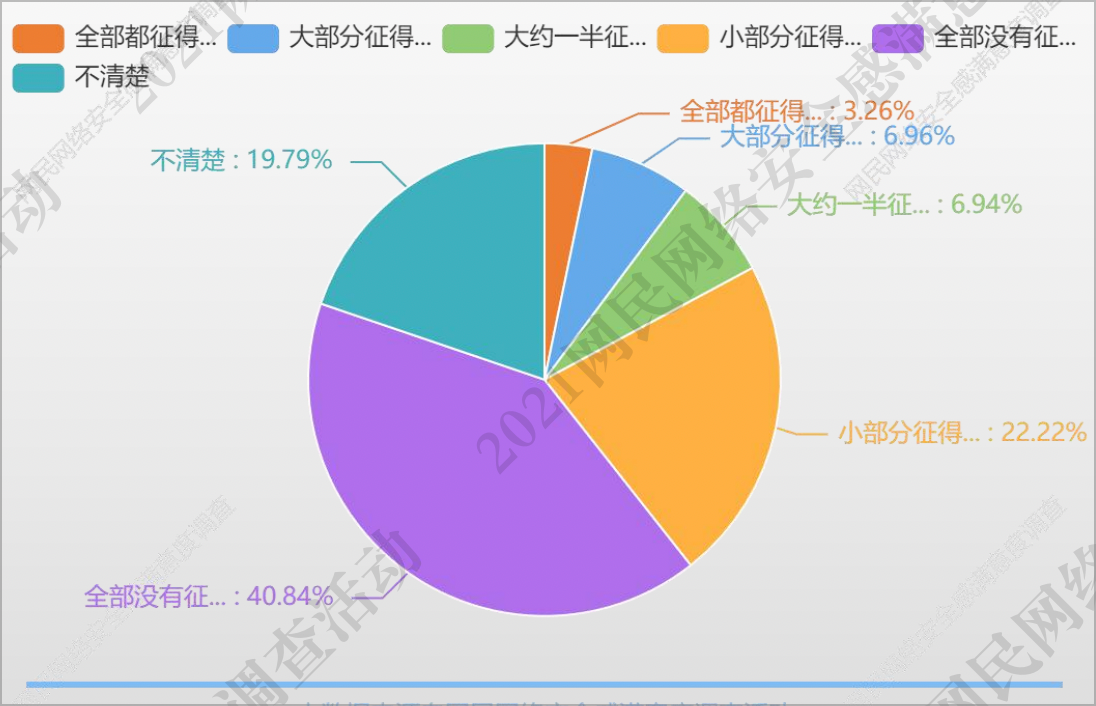
1. 公众网民认为APP存在多种违规收集个人信息的问题

60.12%的受访群体遭遇过APP收集与功能无关的个人信息，57.78%的受访群体遭遇过APP频繁索要无关权限，50.25%的受访群体遭遇过APP强制索取无关权限，不授权就闪退，50.02%的受访群体遭遇过APP默认捆绑功能并一揽子同意。



1. 公众网民对精准广告推送的看法

约九成网民在日常上网时收到过精准广告，约一成网民很少或者没有收到过精准广告。在广告推送的过程中，四成网民表示网络服务经营者全部都没有征得同意即向用户发送广告；超过两成网民表示经营者大部分都没有征得用户同意；还有两成网民不清楚发送广告是否征得过其同意。



1. 调查结果分析
2. 目前隐私泄露在公民日常生活中出现的频率高、范围广，并且大部分公民都能意识到自己的个人隐私数据被泄露（只有不到10%的公民对个人隐私数据泄露感到无所谓）
3. 公民认为社交应用类网络服务的个人信息风险最高
4. 公民认为手机APP是个人隐私泄露的重灾区，并认为大量APP存在强制违规收集与功能无关的个人信息，尤其是注册APP是的强制权限索取（甚至不同以就闪退），可见国内APP对于隐私数据的收集方面是存在很大问题的。
5. 大部分公民都收到过各大购物APP发送的精准广告推送，并且此类广告推送所需的数据收集服务均未经过公民的同意。
6. 大数据时代隐私泄露问题的伦理保护难点
7. 大数据时代，个人权利和个人隐私保护存在天生的矛盾性

比如疫情时代，政府在使用大数据技术来完成公共服务、优化决策时，如疾病防治、公共交通等，就有时需要以牺牲大量个人隐私为代价，以获得具体决策以保证公民的人身安全。这种一方面要求保护个人隐私；另一方面又要求搜集海量个人数据的悖论需求，确实是的政府难以兼顾个人隐私的保护和个人权利的保证，往往都是牺牲个人隐私以保护个人权利。

1. 互联网大公司的数据垄断严重影响了社会公平

如上文的调查结果分析，各大互联网公司的收集APP是个人隐私泄露的重灾区，它们会索取大量与功能无关的相机、位置隐私权限，但用户不知晓其收集这些信息是为了什么服务，这种数据富有者对数据少有者的信息垄断就是某种程度上的信息霸权。如果缺乏市场、政府以及相关法律的监管，企业能轻而易举，在不知不觉间地掌握个人的行为、思想。

1. 普通人应该如何应对大数据时代的隐私泄露

信息时代的发展不可能离开掌握了数字信息技术能力的人，缺乏基本信息技术能力的人很可能会陷入信息贫困，进而导致收入贫困、人类贫困。因此对于我们普通人来说，学会如何应对大数据时代的隐私泄露就相当重要了（至少能免去相当程序的个人隐私泄露）。

1. 网上冲浪切勿使用真实姓名、真实生日
2. 对于互联网上涉及个人信息的调查问卷一律不填
3. 微信、qq等通信软件的密保手机号能不绑定就不绑定
4. 尽量使用密码支持、拒绝面容支付（杜绝生物信息的收集）
5. 总结

大数据时代隐私泄露伦理问题的出现不是短时间内产生的，而是原有互联网发展初期隐私保护伦理问题的演变。这些问题导致了个人利益与公共利益之间的困境，进一步影响到了社会的公平性。伦理问题的出现不仅是由于大数据技术自身逻辑的缺陷，也是由于新技术与旧有伦理规范不相适应，各参与主体隐私保护伦理意识缺乏所引起的。解决这些伦理困境需要从责任伦理的角度出发，关注大数据技术带来的风险，倡导多元参与主体共同努力，遵守大数据时代隐私保护伦理准则，加强道德伦理教育和健全道德伦理约束机制。

1. 参考文献
2. 佟少耕，大数据时代，个人信息保护实案分析
3. 陈根，大数据时代下的隐私悖论，隐私危机来自哪里？
4. 中国政法大学，个人信息保护和数据安全网民满意度调查报告(2021)
5. 张峰，《学术前沿》2019年8月上