

On the Security of Personal Information in the Era of Big data

Ying ZHOU Zhengde BAO Yawen TANG

School of Computer and Software, Jincheng College, Sichuan University, Chengdu, 611731

Abstract

Big data era is the accumulation of highly information construction, mobile Internet, in-depth learning, artificial intelligence and a series of new technologies for the future human pursuit of personalized life has created possibilities. But at the same time, the user's personal information has also been violated, and the legitimate rights and interests of the user have been damaged. This paper summarizes the concept of big data and personal information, analyzes the current situation of personal safety information in big data era, and puts forward some measures.

Key Words

Big Data, Personal Information Security, Personal Privacy

DOI:10.18686/jsjxt.v1i2.718

浅析大数据时代下的个人信息安全

周颖 鲍正德 唐娅雯

四川大学锦城学院计算机与软件学院, 四川, 成都, 611731

摘要

大数据时代是高度信息化建设堆积而成, 移动互联网、深度学习、人工智能等一系列的新技术为人类未来追求个性化的生活创造了可能, 但同时用户的个人信息也遭到了侵犯, 用户的合法权益受损。本文概述了大数据及个人信息概念, 浅析了大数据时代下个人安全信息现状并针对性的提出了措施。

关键字

大数据; 个人信息安全; 个人隐私

1. 引言

在日常生活中, 个人的电话号码、住址等隐私信息在无意识的状态下可能被银行等机构泄露的情况屡见不鲜。突然接到的陌生电话可能是售货员售卖商品, 可能是假装亲戚勒索钱财, 也可能是考证机构推广课程。在经历诸如俄罗斯的“窃听门”、Facebook 的“泄露门”等事件后, 大多数人敲响了对个人隐私保护的警钟, 自身防范意识不断加强, 同时个人信息安全问题也引发了众多讨论。

2. 大数据与个人信息安全概述

2.1 大数据概述

“大数据”最早源于美国, 因其海量的数据规模、快速的数据流转、多样的数据类型和较低的价值密度引领

人们走进了数据的世界。^[1]大数据在各国的发展大同小异, 根据各项调查数据报告显示, 2018 年我国大数据规模相较 2017 年同比增长 30%, 同时《大数据安全白皮书》显示 2019 年我国的大数据市场产值将达到 8000 亿元。大数据带来的影响不仅停留于国家层面和数据的展示, 而且通过多种形式深入了人们的生产生活, 高校学生信息统计、企业营销策略分析、软件智能个性推荐都和大数据息息相关。

2.2 个人信息安全

“个人信息安全”涵盖内容宽泛, 包含公民的身份证号、个人财产、家庭信息等较为隐私信息的安全状况, 信息安全虽受国家政策保护, 但仍因各种钓鱼网站频出、黑客攻击、社交媒体强制绑定手机号等违法行为而导致

公民的个人信息面临被窃取、泄露以及出售的危险。

3.大数据时代下个人信息安全的现状

3.1 采集过程中对个人信息的侵犯

在这个信息飞速发展的时代,用户的一举一动都受到了隐形的监控。用户通过浏览器点击的每一个新网页都会被实时记录并转化为数据,定位到此台设备上,为后续大数据计算提供决策支持。在这一过程中,一些平台的 cookie 中使用模糊词组,对用户没有明确的说明;且用户也没有制止这种侵权行为的方法。

用户在安装手机软件时会遇到权限管理问题,包括读取用户手机的通话记录、手机联系人、用户的位置信息等等。通过不授权则无法正常甚至不能使用软件的手段强制获取用户权限的行为均侵犯了用户的个人信息安全。在 2019 年中消协《100 款 APP 个人信息收集与隐私政策测评报告》的调查显示手机 APP 软件收集用户个人隐私信息的问题十分严重。过度收集用户信息的问题存在于超九成的手机 APP 软件中,更有甚者,部分金融理财方面的 APP 还有“不承担责任”等不合理条款,^[2]而大多数用户为了正常使用软件通常会忽略这些问题。

3.2 使用过程中对个人信息的侵犯

个人信息在被平台通过不正当手段获取后,用大数据算法来推测用户未来的行动。例如,淘宝总会为用户推送可能喜欢的东西,它就是基于用户性别、年龄、搜索记录、浏览的界面、停留的时间、购物记录等来计算形成一个用户消费数据,根据消费数据进行针对性推荐。平台所推出的个性化服务就在用户的隐私信息的整合基础上计算建模,这是用户以牺牲个人信息所得到的便利。

近年来,一款支付软件的年末统计十分的火热,用户通过软件了解到一年内的消费内容等详细信息,然后再分享到社交媒体上,却有极少数的用户反思为何记录的如此详细。支付平台通过分析用户的消费数据,构建数据网,并推送给用户;得到这些信息的代价就是用户的真实姓名、银行卡、电话号码、身份证号等,或许在未来的发展过程中,最了解用户的不是用户本人而是大数据计算。等用户真正意识到个人信息安全受到窃取时,已很难行使合法权益维护了。

3.3 储存过程中对个人信息的侵犯

信息泄露是存储过程中对个人信息的侵犯的关键点。平台通过安全技术对存储在服务器上的用户的个人信息进行保护,但目前平台的安全技术有限,使得管理难度增大。

3.3.1 小米论坛的注册用户信息泄露

2014 年小米论坛近八百万的用户资料被泄露,疑似在黑客界被传播。而拥有这些泄露的数据可以直接访问用户的手机,获取用户的位置、信息、照片、网上支付账号甚至可以操控用户的手机。

3.3.2 美国共和党的数据库泄露

在 2017 年美国发生了一起大规模的信息泄露案件,共和党 2 亿选民的个人信息外泄导致了社会舆论的沸腾^[3],国民纷纷要求数据信息必须要有安全管理机制,以降低风险。

3.3.3 Gemalto 公司《数据泄露水平指数报告》

根据 2017 年的数据报告分析发现数据泄露问题日趋严重,在 2017 年上半年数据的泄露数量就完全超过 2016 年全年的泄露量^[4]。相当于每秒就有近百条信息泄露,泄露信息涉及政府、金融、娱乐众多领域。在泄露信息区域分布上,北美地区占主导地位。

3.3.4 我国《大数据安全白皮书》

我国在 2018 年的《大数据安全白皮书》调查中反映出数据泄露中最主要的攻击手段是黑客攻击其次是恶意软件。大数据在没被提取分析之前数据量大且杂乱从而难以保证安全性,入侵者通过特殊程序进入各数据库、获取用户个人信息。

4.大数据时代下个人信息安全的保护措施

4.1 加快个人信息安全法律法规的制订工作

保护公民的个人信息最强硬的方法就是国家制订法律,通过法律的强制性实施来保护公民的合法权益。

4.1.1 《法治蓝皮书》的发布

2009 年,中国社会科学院曾发布《法治蓝皮书》,

指出目前我国个人信息安全问题面临严峻的形势^[5],立法保护公民合法权益也显得愈发迫切,这也是我国最早明确提出要对个人信息安全进行立法的文件。

4.1.2 法律的间接保护

目前,我国主要分为个人信息的直接保护和间接保护,但都是在特定的领域内,例如在《中华人民共和国护照法》中,这个文件对应的是与护照信息有关的内容,没有以个人信息安全为主体的法律法规,缺乏专门性和统一性。且目前我国的还没有专门的法律出台,在信息安全方面的立法是严重缺乏的^[6]。

4.1.3 数据安全法提案

2019年第十三届全国人大二次会议中许多人大代表提出要出台法律以保护个人信息。在这次会议上,联想的董事长杨元庆就提议,要尽快出台信息安全法,形成更加完整的法律体制。制定法律首先应当明确属于公民个人信息的内容,并规定特定内容不能为他人所传播,否则即触犯法律;其次,对于需采集个人信息的平台赋予明确的权利和限度;最后,制定专属法律,严厉打击采集或存储数据企业出售信息等违法行为。同时也可以通过立法来明确数据在法律上的财产,并根据划分的不同层次来规定对这些信息数据的所有权,各个层次确定所使用及支配的数据范围,进而解决个人信息安全问题。在出台大数据立法项目的同时,也可以将有关人工智能、互联网深度学习等一系列新技术的信息安全问题列入立法内容中。先对这些项目进行深入调查,制定相对应的法律政策,公民利益得到最大限度的保障。

4.2 加强对行业的监管及行业内部的自律

加强对行业的监管及自律包括两个方面,第一是政府要加强对行业内部的监管,第二是行业平台要严于律己,平台方要增强责任感。政府要提高对APP上架的标准,加大对于违法违规申请权限、收集用户个人信息的APP运营公司的监管和处罚力度。

保护个人信息安全最直接的方法就是平台方加强对数据管理的责任感,首先平台要提升技术水平,为数据存储提供安全的空间,同时针对用户的日常进行分类管理,全力保护用户的个人信息,使用户能够拥有更多的选择,为用户提供更优质的服务。平台强化数据管理的责任相比较于国家出台的法律法规更具有灵活性,时

代在不断的发展,市场也在千变万化,加强平台的责任感更有利于保护个人信息安全。

4.3 加强人才培养、提升数据存储技术

目前,基本上所有的大公司的服务器维护费用极其高昂,因而这些公司通过出售个人信息,以维持公司运转。要保护数据安全,维护用户的个人信息就必须突破现有的存储技术,找到更加优秀的数据存储方法。

我国的技术水平处于较高位置,而量子保密通信网络技术目前是解决信息安全最好的技术手段。它是一种较为安全信息传送技术,现如今在国家科技、政治等领域都有着举足轻重的作用。国家需大力培养技术人才,更好的维护用户权益。

4.4 加强个人信息隐私的保护意识

在大数据时代,只要操作电子产品就能产生许多与自身相关的数据。智能设备、社交媒体、视频监控、购物平台,无时无刻不在记录用户所产生的数据,平台通过这些数据的汇总,产生用户本人的关系网,用户的信息一览无余,甚至还能推测出用户的下一步需求。在现实生活中不使用电子产品显然是不切实际的,因此需要用户提高安全意识,注重保护自己的隐私。用户在提供个人信息的同时要明确并辨别信息的内容及价值。放弃互联网所带来一定程度的便利,更加注重安全问题。国家相关部门调查显示,虽然大多数的用户认为滥用个人信息可以申请赔偿,但却不知道某些收集个人信息的行为是可以直接不接受的。用户应学会分辨大数据时代信息的正误,取其精华去其糟粕,用敏锐的自我保护意识维护自身的合法权益。

5. 结束语

大数据时代的到来加速了社会发展的脚步,进而更好的为决策者提供更加优质的决策,进而提高生产力和效率,让人们生活更智能、更便利。我们在认可大数据的优势的同时注重个人信息安全保护,政府方面可加强个人信息泄露犯罪打击力度,企业方面可强化数据平台技术监管,个人方面可加强自我保护能力,多方携手才能使大数据的优势发挥到极致。

参考文献

[1] 张兰廷.大数据的社会价值与战略选择[D].中共中央党

校,2014.

[2]张世祥.第三方网络支付安全中的责任分配探析[D].
中国矿业大学,2018.

[3]刘勃然.21 世纪初美国网络安全战略探析[D].吉林大
学,2013.

[4]李明选.互联网金融产业及其对传统金融冲击影响的
研究[D].上海社会科学院,2015.

[5]蔡泉水.新媒体环境下我国主流意识形态安全研究
[D].南昌大学,2016.

[6]刘旭辉.互联网金融风险防范和监管问题研究[D].中

共中央党校,2015.

作者简介

第一作者:周颖(1997-),女,汉,河南省洛阳市,
本科,四川大学锦城学院,研究方向:大数据应用与商
业智能。

第二作者(通讯作者):鲍正德(1989-),男,汉,
黑龙江哈尔滨,研究生,四川大学锦城学院,研究方向:
电子商务。

第三作者:唐娅雯(1999-),女,汉,四川省资阳市,
本科,四川大学锦城学院,研究方向:信息管理、J2EE