# Impacts of user information use and distribution to third-party companies LaTeX

Panupong Leenawarat[1*] and Anna R. Napoleone[1†]

[1]Computer Science, University of Massachusetts Amherst, Amherst, US.
[*]Corresponding author. Email: pleenawarat@umass.edu
[†]Mentor.

**Abstract**

The United States is a country that prides itself on property rights. It has been questioned who can control their personal information on the Internet. As studies on big data of users' personal information become more prevalent, the frequency of lawsuits is increasing. In fact, our privacy has become a product that can be bought, sold, and shared. We could learn the impacts of personal data misuse in order to prevent negative outcomes.

## 1 Introduction

Analysis from big data of users' personal information can provide knowledge that can get significant value from it and identify new opportunities in business. However, the idea of "acquisition of user data" has created controversy when our privacy has become a product that can be bought, sold, and shared. In some cases, people think that this exchange impacts individual privacy. In the US, there are many privacy issues related to the use of personal information for third parties' research or analytic without individual consent. It creates tension between the use of third-party experimentation and user privacy. For instance, some believe that individual privacy was violated when Facebook ignored the fact that Cambridge Analytica misused personal data to give to dishonest advertisers. The advertisers can target their advertisements to a person with a sensitive personality. Thousands of users consented to have their data collected. However, personal information of more than 87 million Americans was harvested without their awareness. Today, there are still few laws in US that can protect the victims in the event that privacy and personal information from being stored or distributed for any purpose, including the use for denial of insurance or employment.

# 2 Background

## 2.1 Personal Information

Under the Children's Online Privacy Protection Act (COPPA), a law to protect the privacy of children under the age of 13, and Federal Trade Commission(FTC), the following is considered personal information:

- Personal information like name, date of birth, physical address, telephone numbers, email address, and geolocation
- User data like photos, audio files, hobbies, interests, and screen names
- Persistent identifiers, like IP addresses and a device serial number

## 2.2 Uses of Personal Data

In situations of commercial purposes, obviously, companies like Google and Facebook have been selling and sharing user data on their platforms. Sometime it is more than just targeted ads. For instance, Patricia Garcia, contributors of "Your Internet Search History Will Soon Be Up for Sale—Here's How You Can Protect Yourself," state that "companies have realized how lucrative it is to sell user data and they've moved beyond sharing sensitive information with just marketers. This data is now being sold to financial companies, insurers, real estate agencies, car companies, even political parties. [1]"

## 2.3 Information Leakage

Ram D. Gopal et al, author of the research article "How Much to Share with Third Parties? User Privacy Concerns and Website Dilemmas," write to emphasize the problem of privacy concerns surrounding information leakage [2]. "The most familiar sharing mechanism involves the use of cookies, but other more sophisticated approaches exist as well. This sharing of user information with third parties is typically done without explicit user consent or appropriate disclosure mechanisms" (144) [2]. A third-party company can conduct research on a victims' personal information collected and archived in the organization without outlining to the person. In an October 2015 study of over five thousand smart phone applications, administered by IMDEA Networks Institute, a research organization, "more than seventy percent of smart phone apps are reporting personal data to third-party tracking companies like Google Analytics, the Facebook Graph API or Crashlytics. [3]" It shows that it is almost impossible to build an application without integrating external services.

## 2.4 Lack of Laws to exercise control over personal data

According to Daniel J. Weitzner, who wrote the technology forums at Lawfare "How Cambridge Analytica, Facebook and Other Privacy Abuses Could Have Been Prevented," the law is ambiguous [4]. Cambridge Analytica has been illegal and the Federal Trade Commission could have taken an action to the prohibited practice if laws and regulations were legislated. Weitzner was disappointed

that Congress declined to act on the Consumer Privacy Bill of Rights' proposal five years ago; therefore, "it never became a law. [4]" The Consumer Privacy Bill of Rights would have allowed an individual to have right to exercise control over what personal data that companies collected from the person and how they use it. Weitzner assured that "Under that legislation, the conduct of both Facebook and Cambridge Analytica would have been illegal and the Federal Trade Commission could have stopped or deterred it with clear prohibitions and fines. [4]"

### 2.5 Privacy vs. Technologies

On the other hand, many companies have expressed concerns about "stifling innovation with overly burdensome rules." Weitzner also says that "Continued innovation must be encouraged—but not at the expense of leaving citizens in fear of being swept into out-of-control commercial or political experiments." The limits of personal data usage regulation need to be "the right balance between the protection of individual's personal data and the freedom of economic actors to take the advantage of the opportunities provided by new technologies," according to Isabelle Falque-Pierrotin, president of France's Commission Nationale de l'Informatique et des Libertés (CNIL), the country's independent data protection authority [5]. Falque-Pierrotin says that "Currently, there is a clear imbalance between individuals online – internet users – and web companies that use their data. [5]"

## 3 Why Our Information Matters

Corporate competition to accumulate personal information leads to smarter business moves, higher profits and more efficient operations, especially happier customers. According to Emily Steel, who wrote the article "Companies Scramble for Consumer Data," companies create algorithms and feed users' information to determine and predict customer behavior [6]. In a study of general information about a person, administered by Emily Steel, age, gender, and location are worth a mere $0.0005 per person. Those who are shopping for a car, vocation or a financial product are more likely to reach $0.0021 per person. Moreover, in a situation of commercial competition, Steel argues that it can create an unfair competitive advantage in business because "few laws exist in the US that protect the privacy of an individual's data. [6]" Giant corporations have become extremely savvy at finding ways to avoid privacy regulation when they misuse user data while small industries cannot afford to hire good lawyers.

## 4 Approach to Ethics

Collected user data is always accompanied by personal information containing specified patient identifiers. While the information is more intimate, it has more value. The information has become a unique and irreplaceable research raw material which marketers and analysts are willing to pay more to reach specific targets. Furthermore, the advent of affordable technologies which increases the identifiability of personality traits plus a patient's name in research databases has been questioned concerning patients' privacy. As a consequence, people have started to fear that private information

can be used as a basis for discrimination in health care insurance, employment, credit bureau and education. In the case of Disney v COPPA, Disney is sued for violating a privacy protection law that Disney' apps have collected personal information of children under the age of thirteen. Allegedly, Disney's app contains embedded third party software that collects and discloses user information without parental consent. Disney could have been charged tens of millions of dollars in penalties. However, COPPA only focuses to protect the privacy of children under the age of 13, not all ages. In the case of Facebook-Cambridge Analytica, Matthew Rosenberg et al, reporters at the New York Time, "The breach[data leak] allowed the company to exploit the private social media activity of a huge swath of the American electorate, developing techniques that underpinned its work on President Trump's campaign in 2016. [7]" It is obvious that Disney Case, Facebook Case and other cases such as InMobi and FTC, InMobi's application developers collected geolocation data without the consent of users, all involved lawsuits concerning claims of private ownership of personal information used by third-party companies.

# 5 Conclusion

The United States is a country that prides itself on property rights. It has been questioned who can control their personal information on the Internet. As studies on big data of users' personal information become more prevalent, the frequency of lawsuits is increasing. Unfortunately, in 2012, Congress declined to act on the Consumer Privacy Bill of Rights' proposal which would have allowed consumers to have a right to exercise control over their personal data. However, this needs to be reconsidered in the future. Although, in the last decade, the evolution of regulations has imposed limits on the ability of researchers or companies to use personal data, the US still lacks comparable regulations. Laws should be created specifically toprotect the privacy of users and to limit uses of personal information by third-party firms. Finally, as the guardians of information obtained from users, we need to reconsider the laws to answer the question: Who should have ownership over personal data that companies collected.

# References


[1] P. Garcia. (Jun. 5, 2017). "Your internet search history will soon be up for sale-here's how you can protect yourself," [Online]. Available: `www.vogue.com/article/internet-privacy-fcc-laws-eliminated-protect-yourself` (visited on 03/20/2018).

[2] R. Gopal, H. Hidaji, R. A. Patterson, E. Rolland, and D. Zhdanov, "How much to share with third parties? user privacy concerns and website dilemmas," *MIS Q.*, vol. 42, 2018.

[3] I. N. Institute, "7 in 10 smartphone apps share your data with third-party services," *ScienceDaily*, Jun. 9, 2017. [Online]. Available: `www.sciencedaily.com/releases/2017/06/170609103834.htm` (visited on 03/20/2018).

[4] D. J. Weitzner, "How cambridge analytica, facebook and other privacy abuses could have been prevented.," *Lawfare*, Apr. 6, 2018. [Online]. Available: www.lawfareblog.com/how-cambridge-analytica-facebook-and-other-privacy-abuses-could-have-been-prevented (visited on 03/15/2018).

[5] I. Falque-Pierrotin and B. Joyeux. (Mar. 16, 2018). "Protecting data without stifling innovation: A question of regulation?" [Online]. Available: www.greeneuropeanjournal.eu/protecting-data-without-stifling-innovation-a-question-of-regulation/#_ftnref2 (visited on 03/20/2018).

[6] E. Steel, "Companies scramble for consumer data - ft.com," *Financial Times*, Jun. 12, 2013. DOI: ig-legacy.ft.com/content/f0b6edc0-d342-11e2-b3ff-00144feab7de#axzz5CBcU3DLI.

[7] M. Rosenberg, "How trump consultants exploited the facebook data of millions," *The New York Times*, Mar. 17, 2018. [Online]. Available: www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (visited on 03/15/2018).