Topics Related

神楽坂エル, [11.04.21 22:22]

Focused topic: Abuse of personal data tracking in modern internet giants

神楽坂エル, [11.04.21 22:22]

RQ:What does the abuse of personal data tracking bring and how does it affected our daily life

神楽坂エル, [11.04.21 22:22]

Sub Questions:

1. Why is privacy so vulnerable in modern internet?

2. To what extent the internet giants have our personal information, and why do they need these information

3. What is the necessity that we shall protect us from abuse of data tracking

4. What is the future of the relationship between individual and multi-national (internet) companies who have the absolute power of over the internet

Outline

Intro.

arising concern => necessity of law => FLoC example => GDPR intro. + antitrust law => further discussion, moral aspects

antitrust law =>

Laws for Internet Industry Regulating Data Collection is Necessary

Internet companies are chasing your data as if rushing for gold. Your data is being collected, processed, and then abused when you are mostly unaware, in the modern Internet world full of third-party tracking and surveillance programs. Is it common that once you tweet some photo of your delicate Italian flavored lunch and the next day the ads in the webpages and apps become all about pasta and spaghetti sale on Amazon? That is how efficient and excessive the data collection machine is running. To avoid wild and excessive data collection, initiative and idealism are not sufficient, and it depends on the capable laws to make it transparent, controllable, safe, and fair.

There is no free lunch. Data is also money; the data industry is indeed a serious business. As the consumers are enjoying convenient services for low monetary fees or even completely free, their data is gradually collected as an implicit expense for the service. Third-party trackers will notify the companies of what you clicked, posted, liked, watched, listened and

where you went, to generate your personal portrait at their ease. Often such a tracker in the real domain is limited by physical conditions, and without a doubt is considered dangerous and offensive, against real privacy laws, but is seldom saliently perceived in cyberspace. It may be due to the short period from the point the business paradigm shift emerged to monetize the value of data, and the consequential lack of experience of governments and policymakers to deal with virtual privacy, together with the unawareness and ignorance of the end-users like you and me, of such a collecting process that endures along using modern electronic devices, applications and Internet facilities like the Android phones, the Chrome web browser, and the Google search. However, there is an arising ethical and legal concern among the consumers nowadays to the excessive collection of personal data in the recent years, which exhibits the booming trend of the demand of more comprehensive laws from people to protect ourselves. Recently the announcement of FLoC from Google (W3C, 2021) in its popular web browser Chrome has raised an intensive controversy (Cyphers, 2021) among the Internet community and users, and its replacement instead of traditional cookies are recognized as the next strategic step of the advertisement giant towards personal identification against GDPR and further incoming privacy laws. As Google hypocritically clarifying the privacy-friendly policy adopted after the cookies fade out (Clark, 2021), it has been found that the proposed new tool is yet another tracking identifier, even more aggressive and gains more of your interests.

These efforts boycotting immoral and illegal data collection cannot be fruitless, and the Internet giants are not going to be tolerated and unlimited forever. Laws and regulations are to be purposed. In 2020, the ever-so-strict law came ardently welcomed by the EU people, namely the GDPR (Houser and Voss, 2018), and it confined the casual and wild situation of the data collection, and soon it billed Google for a large sum of money up to 4% of the profit a year, namely 400 million euros. You may have noticed that recently the websites often inform you about the cookies they used and require your consent and acceptance, and this broad privacy enhancement is due to the tighten privacy policy adopted in the GDPR. The spirit of GDPR is the awareness and controllability, and the platforms and companies gathering information from the consumers are obliged to explicitly display the data trackers to the user and allow the user to choose among them and offer the detailed list of the data collected if the user requires a transparency report, which makes a giant leap for mankind in the privacy protection aspect. Following the epochal proposal of GDPR as an exemplary attempt, the governments outside of the EU are also evaluating new data privacy laws. (ref…)

On the other hand, the more data the companies store, the more threat your data is under. Data leakage is the Achilles' Heel of the massive data collection. Imagine the database of some third-party tracker providers is hacked and your data is exposed to the hackers or even the public, and such cases are very common to an extent that, numerous zero-day back-doors and exploitation appear publicly per week and more privately utilized and traded on the vulnerability underground market (Ablon et al., 2014) and people heard about websites' database leak more than once a month. Also given the condition that your data is gathered in detail and these data is stored very "safely", that the cloud storage is dispensed in several backup data centers, your data is however under real risk not from the data loss but the vulnerability from vicious hackers, and the more backup copies they store, the more prone to leak your data is. And such leakages are so common that a database consisting of over 500 website leaks, including the recent leak from Facebook of 509,458,528 account info., is built to record known password leaks to remind users whether their password has been compromised (Hunt, n. d.), and an illegitimate industry that involves selling leaked personal data has emerged and long persisted in China as reported (Zhang et al., 2021). Laws and regulations against the underground market of data collected are yet necessary to victims of data leaks.

For advertisement service providers (e.g., Google, Facebook, etc.), data is money and therefore forms a market and industry. If there is business unsupervised, there will be dominance, and if there is a market unsupervised, there shall be an antitrust law to limit the wild growth of capital. Data privacy laws take care of you in the individual aspect, as the competition laws review this problem from the perspective of inappropriate conditions in the business. Robertson analyzed the massive and overdone gathering of personal information, in a perspective of not the conventional data privacy protection law but the competition law of the EU (Robertson, 2020). To apply antitrust concerns, later he justified the definition of the data market, emphasizing the monetary value, although the standard of which is vague for personal data. Following his discussion, the excessive data collection could therefore be interpreted as an abuse of monopoly in a way of either an inappropriate price (in the way of monetized collected data) of products exceeding the actual efficacy of the product or unfair trading condition triggered by the additional data exclusive to the competitors. Although the Internet environment of China is different from those of the EU or the U.S., the phenomenon of web dominance in China is also substantial, that the domestic giants like Tencent, Bytedanace, and Alibaba have implanted their information platform into almost everywhere at which someone can access to the Internet, leading to yet another kind of dominance, of the novel ability to collect data from the IP (Intellectual Property) in their control, except the aforementioned dominance of unfair price and trade condition. In the recent antitrust case of Alibaba(The State Administration for Market Regulation imposed administrative penalties on Alibaba's "two-for-one" monopoly, 2021), China government has recently realized the harm of dominance in the Internet capitals but is still ignorant that the cause of such dominance relies upon the monopoly of the right to speak and to collect data in the virtual domain, and the only a concrete competition law in the Internet industry will refrain the problem of the excessive and inappropriate gathering of data of the information industry.

It was the best of times, it was the worst of times (Dickens, 1859). The age has witnessed the tremendous booming industry of the Internet and the grand revolution in productivity and economics. The age has also seen the spirit of free, open, decentralized, crowd-sourced Internet failing in front of the capital flowing in, and the fall of him who fights with monsters of Internet monopoly. Namely Google, the challenger of Microsoft who once owned the largest entrance of Internet, the Internet Explorer, advocating its free idealism of Internet is now yet another tyrant of the web, dominating. When idealism and initiative fail, laws and regulations shall come about, especially for data privacy. So far, there is still an enormous gap of law and regulations between the real world and the virtual world, since the equivalent part of the virtual world could not be simply found or does not exist at all in the material world. Hence it’s necessary and important for policy-makers to set up solid statute law against excessive and inappropriate data collection in the virtual domain.

(Total Words: 1406)

References

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data: Hackers' bazaar. *Rand Corporation.*

Houser, K. A., & Voss, W. G. (2018). GDPR: The end of Google and Facebook or a new paradigm in data privacy. *Richmond Journal of Law & Technology*, 25, 1.

Robertson, V. H. (2020). Excessive data collection: Privacy considerations and abuse of dominance in the era of big data. *Common Market Law Review*, *57*(1).

Cyphers, B. (2021). Google's FLoC Is a Terrible Idea. *Electronic Frontier Foundation.* Retrieved from https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea

Clark, M. (2021). Google promises it won't just keep tracking you after replacing cookies. *The Verge.* Retrieved from https://www.theverge.com/2021/3/3/22310332/google-privacy-replacing-third-party-cookies-privacy-sandbox

Xiao, Y., & Karlin, H. (2021). Federated Learning of Cohorts. *W3C Community Group Draft Report.* Retrieved from https://wicg.github.io/floc/

Hunt, T. (n. d.). Have I Been Pwned? Retrieved from https://haveibeenpwned.com/

Zhang C., Li J., Sun Z., Zhang M., Liang J., Guo J. (2021), Three Questions to Data Leaks Part I: Why Leak? Billions of Personal Data is Abusively Sold with Clearly Shown Price. *Xinhua News Agency*. Retrieved from https://baijiahao.baidu.com/s?id=1697435347254228705

Dickens, C. (1859). A Tale of Two Cities. New York, NY: Penguin Group.

The State Administration for Market Regulation imposed administrative penalties on Alibaba's "two-for-one" monopoly (2021). *Economic Information Daily*. Retrieved from http://www.jjckb.cn/2021-04/12/c_139874650.htm