COMPETITION TO COLLECT AND MONETIZE PERSONAL INFORMATION[1]

Four forces are creating more opportunities for high-tech firms to collect personal information:

1. **Ongoing innovations are expanding consumer use of the internet for shopping, payments, banking, video, communications, medical care, etc.**
2. **The advance to 5G will connect (a) more people to more devices, and (b) more devices to each other. The build-out of the *Internet of Things* (IoT) will generate data from more sources.**
3. **The most successful platform companies have expanded their services into payment systems, internet infrastructure, supply chains, product distribution, and even into healthcare, agriculture, and manufacturing.**
4. **Artificial Intelligence (AI) is improving the efficiency of efforts to develop more accurate profiles on individuals.[2]**

With these powerful forces, many predict that personal information and the profiles developed from the information will become a new asset class. For this prediction to hold, firms must be able to monetize the information they collect.

1. INTRODUCTION

There are two primary ways to monetize personal information: (i) use the information in your own marketing, and (ii) sell the information to other firms seeking to improve their marketing.[3] Whether efforts to monetize data would make sense depends, interestingly, on what firms gain by promising not to collect and monetize personal information. Consumers may be attracted to firms that credibly commit to not collect personal information. In effect, by not collecting and monetizing, some firms may earn additional profits.[4]

---

[1] This brief has been prepared for Yale School of Management Economic Analysis of High-Tech Industries class, August – December 2023 by Aneta Gasiewska, Jakub Madej, and Edward A. Snyder.

[2] As stated by Coursera's Andrew Ng, "As artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed." Feb 10, 2020.

[3] These two are not mutually exclusive and some companies will do both. Such is the case with telecommunications companies such as Verizon, Deutsche Telekom, and Telefónica. They have achieved internal monetization by using data to optimize operations and client services, and they also leveraged that data, anonymized and aggregated, across various use cases for their B2B clients and partners by offering:

- Geotargeting and geofencing for retailers and tourism.
- Traffic flow and density planning for ad agencies, government agencies, public transportation companies, city planners, and health care organizations.
- Fraud detection for financial institutions and credit card companies.
- Smart targeting and click-stream insights for brands and digital advertisers.
- Location, layout, and staff planning for retail stores.
- Internet of things (IoT) applications for a variety of companies.

According to (Gandhi et al., 2018), successful data monetization requires focusing on the highest-value opportunities that are consistent with overall business strategy.

[4] In principle, rights to information could be allocated to the individual, in which case firms would have to compensate

Collecting and monetizing is not, therefore, an "uncontested layup" in basketball terminology. We need to consider which firms are best positioned to develop the most accurate profiles of individuals? The question uses the term "most accurate profiles" because information can be transferred. The "good but not great" profiles will have little use. We also need to consider, among the firms that develop profiles of individuals, which will be able to monetize the information?

By addressing the questions who will win the competition to collect and monetize personal information, we can avoid making the mistake of believing the hundreds of narratives about how individual firms will make huge profits from the information they collect. Those mistaken beliefs should give way to an understanding that, like in most high-tech contexts, only a few firms will be on the leading edge. For other firms, their efforts to collect information will add to costs without increasing profits. Given that highly accurate information is better than pretty good information, it is useful to state the following hypothesis:

> *Hypothesis*: The winners of the competition to collect and monetize information will be few in number. As in much of high-tech, the leading-edge only accommodates a few firms.

In Section 2, we will take a critical look at the claims that firms make about their ability to collect and monetize personal information. After reviewing the data landscape in Section 3, we present in Section 4 a framework for assessing whether firms can develop a competitive advantage based on personal information. In Section 5 we address some regulatory issues. In Section 6 we offer closing thoughts.

2. SHOULD WE BELIEVE ALL THE NARRATIVES?

Should we believe that ride-sharing companies like Uber and Didi will be able to offer targeted investment advice to passengers who are "captive" in the back seat? Is it true that from a single comment on a LinkedIn post or Facebook page that firms using AI will be able to develop an profile of the commenter? Does it make sense that personal information generated by individuals accessing information on the Weather Channel is a highly valuable asset?[5]

Related, should believe the implications of these narratives for individual firm valuations? For large numbers of high-tech firms, lofty valuations are based in substantial part on narratives about collecting and monetizing personal information.

Some of these narratives will prove to be true. Using again a basketball metaphor, some hook shots hit the backboard and go in. But before expecting those firms to be "leading scorers", we should recognize that some firms have already developed robust personal profiles and are positioned on the free-throw line.

---

individuals to be able to collect the information. Conversely, rights could be allocated to firms, in which case, individuals seeking to keep their information private would be faced with the challenge of securing rights to their information. See the Coase Theorem and (Posner & Weyl, 2018).

[5] A recent litigation case against TWC Product and Technology LLC and its parent company IBM questioned whether their Weather Channel app needed to continuously trace the exact location of its 45m users (Berg, 2020). Data collected this way was later on sold to third parties. The case ended in a settlement.

Consider Tencent, the Chinese conglomerate whose WeChat platform has over 1.2 billion users (Statista, 2020). Tencent offers to this massive user base payment systems, music services, web portals, e-commerce sites, mobile and multiplayer online games, internet services and smartphones. A typical user shifts among these functions throughout the day, generating information about their habits, purchases, payments, preferences, and social connections (Barclays Equity Research, 2018). Tencent's position in the competition to collect and monetize information is robust, strong, and improving. Tencent is in a position to know (i) who was on your team's chat last week, (ii) whether your team includes international contacts, (iii) whether team members play games together, and (iv) whether a user sent money to a team member using Ten Pay (Wang, 2018).

Consider also Amazon. Over its history, Amazon has collected information about shopping habits as users search for products. When consumers complete transactions, Amazon also learns about where customers live, whether they have moved, whether they go on vacation, and where friends and relatives to whom they send gifts reside. Amazon learns about what credit cards users own, who is important in their lives, and whether they purchase from a computer or mobile phone. During the Covid-19 pandemic, Amazon could observe whether individuals started a garden, whether they ordered food for home delivery, and, if so, whether they selected a diet food delivery plan, e.g., Nutrisystem. When Kindle users start and stop reading a book or highlight phrases in the e-books they read, Amazon learns yet more. The same applies to when users access Amazon's prime video service. Yet more information is generated by users who ask Alexa, Amazon's virtual assistant, about their next appointment or for a person's contact information. Recent rollout of the Halo personal tracker will yield yet more data.[6]

If you find the Tencent and Amazon examples to be compelling to the point of making it hard to imagine that others stand a chance of winning the competition to collect and monetize information, then you are likely to favor the following hypothesis:

> *Hypothesis*: The most likely winners of the competition to collect and monetize personal information will be the large platform companies with large numbers of users who use the platform for multiple purposes.

This hypothesis leads one to focus on the firms that are already collecting and monetizing information. It also leads one to ask what new platforms will be developed in the future. For example, leaders in autonomous vehicles will be well positioned to collect and monetize information.

3. THE DATA LANDSCAPE

Amounts of data generated by customers and collected by companies has been on an exponential rise over the last quarter of a century. In mid-1990s an average personal computer would store 1GB of data, an equivalent of roughly 160 photos taken by a modern iPhone. Sequencing the first human genome time took thirteen years and produced three gigabytes of data; now 23andMe, a genetic testing company, claims to have data on over ten million customers. According to some

[6] Announced on August 29, 2020, Halo wearable device allows to monitor users' fitness routine, as well as features two new functionalities: mood recognition based on voice recordings and body fat percentage calculator, based on images from a phone's camera (Bohn, 2020).

estimates, new data generated worldwide in 2020-21 will amount to 90 zettabytes, which is more than all the data produced since computers were invented (Siegele, 2020). (One zettabyte equals (1e+12) gigabytes, i.e., a trillion gigabytes.)

An important reason for ever increasing amounts of data is creation of the so-called 'mirror worlds.' As physical items and experiences are simulated in the virtual reality through sensors and wireless connections,[7] new business models, markets and institutions emerge, leading to emergence of 'data economy.'

Giant tech companies – Facebook, Amazon, Apple, Netflix and Alphabet, and Microsoft in US and Baidu, Alibaba, and Tencent in China – have collected vast amounts of customer information and devised sophisticated algorithms to generate insights from them. In China, Baidu, Alibaba, and Tencent oversee most of the digital content. Their impact is comparable to the joint influence of Amazon, Bank of America, Google, Facebook, Activision Blizzard, CNN, and ESPN. By some estimates, Chinese consumers spend 55 percent of their time online within the Tencent digital ecosystem (Whitler, 2019). Cross-platform integration and content-based engagement within a less rigorous regulatory framework allows the Chinese companies to completely redefine interactions with customers, all based on insights derived from customer data.

In contrast to China and the US, the EU lacks pioneers in personal data gathering and utilization. Although individual companies successfully leveraging data to drive customer engagement and introduce new sales models can be found, e.g., Zalando in the eCommerce space and Salisbury's in retail, they are far behind their US and Chinese peers. One exception is Swedish-based music platform Spotify, which leverages AI-powered personalized recommendation algorithms to come up with playlists catering to individual tastes.

Here are examples of how companies use analytics to drive revenues, improve efficiency, increase customer engagement, build brand loyalty or improve operations.

Examples of big data applications	Description
Personalized Recommendation System	▪ Use of a collaborative filtering engine (CFE) to analyze previous purchases, items on the wish list, search history, product review and rating history ▪ Leveraging insights from the network of customers to make product recommendations ▪ Result: revenue increase, e.g., Amazon reported to generate 35 percent of its annual revenue through personalized recommendations (Wills, 2020)
Anticipatory shipping model	▪ Application of predictive analytics to forecast which products are likely to be purchased, when, where and in which quantity ▪ Shipping of products to a local distribution center/warehouse ahead of receiving an actual order from the customer ▪ Model patented by Amazon ▪ Result: decrease `the delivery time and expenses, increase in sales and profit margins

[7] See the brief, *Advance to 5G*, and individual briefs on the implications of 5G for ride-sharing, video-streaming, payment systems, and eCommerce.

Supply chain optimization	▪ Cooperation with manufacturers and suppliers to track inventory levels ▪ Selection of the warehouse/vendor based on proximity and costs to fulfil the order ▪ Optimization of delivery schedules, routes and product mix ▪ Result: a decrease in shipping costs by up to 40 percent.
Price optimization	▪ Dynamic pricing models leveraging big data to provide personalized pricing ▪ Leveraging data on customer's activity on the website, product availability and popularity, history, expected margins ▪ Change in prices even up to every 10 minutes ▪ Result: increase in customer loyalty, profit increase of 25 percent annually
Integrated customer profiling	▪ Deriving insights about customer behavior from diverse sources of data, incl. machine-to-machine communication ▪ Use of individual data on e.g., sleeping patterns, commute time, eating preferences to develop targeted customer engagement ▪ Result: potential for individually targeted interventions (currently untapped)

Source: based on https://www.investopedia.com/articles/insights/090716/7-ways-amazon-uses-big-data-stalk-you-amzn.asp

4. FRAMEWORK

Hagiu and Wright (2020) propose a seven-step framework to evaluate whether data collection can provide a sustainable competitive advantage for firms.

a. How much value is added by customer data relative to the stand-alone value of the offering?
b. How quickly does the marginal value of data-enabled learning drop off?
c. How fast does the relevance of the user data depreciate?Is the data proprietary—meaning it cannot be purchased from other sources, easily copied, or reverse-engineered?
d. How hard is it to imitate product improvements that use customer data?
e. Does the data from one user help improve the product for others?
f. How fast can the insights from user data be incorporated into products?

Based on the Hagiu and Wright framework, the process of data collection and monetization, if successful, involves transforming, enriching, and analyzing raw data into data that can be put to work. Large platform firms that are already succeeding with these steps are the most likely winners of the competition to collect and monetize personal information.

In this light, the surge in valuations of top high-tech firms in the first eight months of 2020 makes sense. Consider the US experience:

> "The five firms, worth $5.6trn, make up almost a fifth of the value of the S&P 500 index of American shares. The last time the market was so concentrated was 20 years ago, before a crash that triggered a widespread downturn. The other, opposite concern is that investors may be right. The big tech firms' supersized valuations suggest their profits will double or so in the next decade, causing far greater economic tremors in rich countries and an alarming concentration of economic and political power." (The Economist, 2020)

More about valuations will be revealed in the years to come. AI technologies are still in their relative infancy. For example, nearly all searches are currently based on words, but searches based on image and video could be far faster, and more accurate:

> "At the moment, self-service checkouts are still relatively primitive: you have to scan the barcode of each product, one by one, but using new machine vision technology based on cameras in the ceiling, the store will be able to 'see' you've picked up a certain box of cereal and charge you for it immediately, and you can just walk out of the store without having to stop by a checkout." (Michael Lippert, portfolio manager at Baron Capital.)

Does data collection justify current high valuations of the tech firms? Some investors believe it does. They point to the untapped potential of machine-to-machine (M2M) communications, increasing automation and forthcoming technological breakthroughs, which will be enabled by 5G communications.

As our personal devices, household equipment and wearables start seamlessly exchanging our data among each other without our involvement, they will trigger massive productivity improvements. Think about the current supermarket experience: although you might have a shopping list app shared with other members of your household and use a self-checkout counter, overall process automation is still relatively low. The arrival of 5G and advances in IoT technology might soon entirely transform the experience: your fridge might automatically order food for you when supplies are low, while a shopping list will be automatically compiled based on the latest nutritional plan from your dietitian. All could be delivered by a drone.

Advances like that will span across the whole economy, from healthcare, through financial services and eCommerce, to travel and entertainment. Because data will be a key enabler, those who have access and know how to use it, stand to gain most. As one analyst said, "We continue to believe Alphabet is undervalued for its growth prospects, leadership position in digital advertising and cash-rich balance sheet." (Neate, 2020)

5. REGULATION

Data collection by tech companies are of interest to regulators and competition authorities. Valuations could be greatly affected by competition policy and regulations concerning privacy.

Regulation in Europe is already in place. Europe's General Data Protection Regulation (GDPR) is considered the world's strongest set of regulations on data protection. In force since May 2018, the framework established individuals as data owners, and put limits on organizations as pertains to data processing. Under the GDPR, personal data includes any information related to a natural person (data subject), which can be used to identify the person. As such, it could be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or even a computer IP address (Kaelin, 2019). Companies handling personal data must limit access to personal data to authorized personnel only. The main underlying principles of GDPR are:

- Consent
  Organizations need to clearly and concisely present their terms and conditions, and any request for consent must avoid any ambiguity. Furthermore, each time organizations handling private or sensitive data want to use them for another purpose than originally granted, they must obtain data subject's permission. There is no such thing as a continuous blanket consent under the GDPR.

- Breach notification
  Once an organization discovers private data has been compromised, it has 72 hours to notify all data subjects that a breach has occurred. Notification can take many forms (email, phone, public announcement).

- Right to access
  Data subjects can request information on what personal data pertaining to them is being processed, where, for what purpose. Organizations processing personal data need to, on request, provide a free electronic copy of the data.

- Right to be forgotten
  Data subjects have a right to withdraw their consent for data processing at any point in time. At that point, organizations need to halt processing, cease further dissemination of the data and erase the data they have.

- Data portability
  Data subjects have a right to receive any previously provided personal data in a commonly used and machine-readable format.

- Privacy by Design
  Organizations must follow Privacy by Design principles and implement measures to protect personal data. In practice, this means that companies process only the data absolutely required for business purposes, and limit access to data among employees.

- Data Protection Officers
  Large organizations (over 250 employees or any enterprise processing the personal data of over 5,000 data subjects in any 12-month period) need to designate a Data Protection Officer (DPO) to oversee the application of the GDPR, as well as to protect personal data from misuse and unauthorized access.

GDPR has exposed big tech's data handling practices that otherwise might not have been apparent to customers. As an example, Amazon's Echo devices listen, record and transcribe conversations held in close proximity of the microphone. In a few cases, data has mistakenly been shared with third parties. In a widely publicized incident from 2018, a German citizen requested that Amazon shares records of his personal data. He received 1,700 audio recordings of alarms, public transport inquiries, music commands and personal conversations of an entirely different person. As it later turned out, the person making the request did not even own an Echo speaker, and only expected records of his Amazon search history (Dobush, 2018).

Other regulatory approaches could be grounded in how property rights are allocated. The Coase Theorem states that if transaction costs are low, market exchange will lead to a Pareto efficient outcome irrespective of the initial allocation of goods. Legal regimes could develop rules by which property rights are assigned to individuals. Given that transaction costs in this context are not zero, such an assignment could affect actual behaviors and valuations.[8]

Of note, as of August 2023 the US Federal Trade Commission is planning to file a lawsuit against Amazon, alleging among other things that users were non-consensually enrolled into Amazon Prime subscriptions and used personal information to favor their own products.[9] For other current regulatory matters, see the *Appendix to this Brief*.

6. CLOSING THOUGHTS

Time will tell which pathways to monetize personal information will prove successful. While some narratives seem more compelling, others make no sense. Ride sharing companies such as Uber or Didi are not going to succeed by offering investment advice. Bike-sharing companies will not be able to use information gathered to target individuals with personalized movie recommendations.

It is more likely that in the immediate term personal data collected on individuals will inform adjacent services to those already used. Payment systems' providers might use data mining to uncover insights allowing them to provide better targeted advertising for investments, mortgages and loans. Music streaming services might be able to identify patterns that will allow composers optimize their next album. Online grocery stores might optimize product recommendations based on what they learn about each household's consumptions patterns.

And who will win the competition to collect and monetize personal data? Most likely those who are already doing it: Tencent, Facebook, Amazon, etc. They can already predict that a family is expecting a baby or that a relationship is likely to break up. They will know even more in the future.

[8] A related approach is to view personal information as a form of labor. Then firms seeking to collect and monetize would be required to compensate individuals for supplying their data (Posner & Weyl, 2018). Whether searching through Google search bar, "liking" photos on Instagram or uploading heart rate recordings from the smart watch, customers deliver valuable datapoints to tech companies, and could be compensated for this 'labor."

[9] https://www.reuters.com/legal/amazoncom-set-meet-with-ftc-ahead-potential-antitrust-lawsuit-source-2023-08-07/, https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-takes-action-against-amazon-enrolling-consumers-amazon-prime-without-consent-sabotaging-their.

Appendix: Further information on regulatory matters

Privacy concerns have been the reason for the European Commission launching investigations into M&A cases. Most recently, a full-scale probe into Google's $2.1 billion takeover of Fitbit has been initiated to determine whether the transaction would lead to the tech giant assuming too much control over online personalized advertising (Horney, 2020). The EC worries that personalized data from millions of wearable devices matched with Google's massive existing data repositories will hinder the ability of other companies to effectively compete in the advertising market, and hinder entrance of new ones. Neither Google's proposal to create siloed data warehouses, nor its assurance that the merger will improve competition in the wearable market, seem to be considered sufficient data protection measures by the EC.

Outside of Europe, data protection regulatory frameworks are much looser. In principle, data property rights would lie with anyone who can collect data, rather than with an individual whose data is being processed.

In the US, there is no single principal data protection legislation. Instead, a system of federal and state level laws defines how the personal data of the country's residents should be handled (*International Comparative Legal Guides*, 2020). The Federal Trade Commission Act (15 U.S. Code § 41 et seq.) empowers the U.S. Federal Trade Commission (FTC) to initiate enforcement actions to protect consumers against unfair or deceptive practices (including, for example, an organization's failure to comply with its published privacy promises, failure to provide adequate security of personal information, use of deceptive advertising or marketing).

On the state level, the most comprehensive data protection legislation is the California Consumer Privacy Act of 2018 (*California Consumer Privacy Act (CCPA)*, 2018). The framework has been modeled after the GDPR and is designed to give consumers more control over their personal information. Some key rights granted to customers by the CCPA include:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information;
- The right to non-discrimination for exercising their CCPA rights.

Even within a seemingly looser regulatory framework, questions about unfair advantage from utilizing personal data and dominant market position arise. In 2020, the US has launched an investigation into potential anti-competitive practices of the tech industry's four most powerful players: Amazon, Apple, Facebook, and Google, on the grounds of the companies having a too big of a size and too much power. Each of the firms has been accused of leveraging the dominant position in the industry to exploit the market, harming democracy, consumers and small businesses (Johnson, 2020). Examples of areas of dominance include:

- Facebook's control of social media platforms (Facebook, Instagram, Whatsapp)
- Apple's and Google's control of mobile app markets
- Google's dominance in search

- Facebook's and Google's control of online advertising
- Amazon's online shopping platform

In China, where the ruling Communist Party of China (CCP) strives to control all aspects of the society, the tech sector has been leveraged as an enabler for constructing a surveillance apparatus. One example is the social credit system, announced as a major policy plan in 2014 (Kobie, 2019). The system assigns ratings to individuals, depending on whether they engage in "good" or "bad" behaviors. According to some observers, if a citizen is caught jaywalking or browsing websites whose content is banned in China, he or she might get blacklisted and denied a loan, banned from purchasing plane or train tickets, or refused a purchase of a property.[10]

Originally communicated to the public as a tool to enable reliable credit scoring in a country with no established banking sector, the social credit system has soon evolved into a giant repository of personal data from public and private sources. Already in 2017 it was reported that through face scanning and a robust system of CCTV cameras, Chinese officials are able to track down an individual across the country within just seven minutes. Recent news reports indicate that even bike sharing companies are selling data to the government, which after combining it with information from other sources can get a pretty accurate view of where an individual lives, where she buys her bread, how often she socializes, etc. (Moody, 2018).

The issue of information asymmetry: who has and uses which data, whether data subjects are aware of the fact that their data being used, remains unresolved in digital economy. Traditional industries have addressed it by establishing mechanisms such as a fiduciary relationship, whereby the information shared is privileged, the fiduciary has a legal duty to protect the interest of the data subject, and she can be held liable for breaching that duty. Classic examples of this are doctor-patient or lawyer-client relationships. It seems reasonable to expect that similar mechanisms are in place when e.g., personal gene testing results or health data from wearable devices are considered. However, to this point neither the GDPR, nor other data protection systems have succeeded in establishing similar mechanisms in data protection.

[10] The truth may be more complicated than that, see https://merics.org/en/comment/chinas-social-credit-score-untangling-myth-reality.

Readings

Barclays Equity Research. (2018). *China Internet: Mobile User Engagement Surges, Monetization Should Follow*.

Berg, L. (2020, August 19). *Weather Channel App Settles LA's Data Mining Suit—Law360*. https://www.law360.com/articles/1302703/weather-channel-app-settles-la-s-data-mining-suit

Bohn, D. (2020, August 27). *Amazon announces Halo, a fitness band and app that scans your body and voice*. The Verge. https://www.theverge.com/2020/8/27/21402493/amazon-halo-band-health-fitness-body-scan-tone-emotion-activity-sleep

California Consumer Privacy Act (CCPA). (2018, October 15). State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa

Dobush, G. (2018, December 20). *How a German Man Wanted His Amazon Data and Got 1,700 Alexa Files—About a Total Stranger*. Fortune. https://fortune.com/2018/12/20/german-amazon-data-error/

Gandhi, S., Thota, B., Kuchembuck, R., & Swartz, J. (2018, November 27). *Demystifying Data Monetization*. MIT Sloan Management Review. https://sloanreview.mit.edu/article/demystifying-data-monetization/

Horney, B. (2020, August 4). *EU Probing Google's $2.1B Fitbit Deal Over Data Concerns—Law360*. https://www.law360.com/articles/1298172/eu-probing-google-s-2-1b-fitbit-deal-over-data-concerns

International Comparative Legal Guides (United Kingdom). (2020, June 7). [Text]. International Comparative Legal Guides International Business Reports; Global Legal Group. https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Johnson, K. (2020, August 1). Antitrust experts weigh in on breaking up Amazon, Apple, Facebook, and Google. *VentureBeat*. https://venturebeat.com/2020/08/01/antitrust-experts-weigh-in-on-breaking-up-amazon-apple-facebook-and-google/

Kaelin, M. (2019, May 23). *GDPR: A cheat sheet*. TechRepublic. https://www.techrepublic.com/article/the-eu-general-data-protection-regulation-gdpr-the-smart-persons-guide/

Kobie, N. (2019, June 7). The complicated truth about China's social credit system. *Wired UK*. https://www.wired.co.uk/article/china-social-credit-system-explained

Moody, G. (2018, December 11). *How Bike-Sharing Services And Electric Vehicles Are Sending Personal Data To The Chinese Government*. Techdirt. https://www.techdirt.com/articles/20181211/02563441198/how-bike-sharing-services-electric-vehicles-are-sending-personal-data-to-chinese-government.shtml

Neate, R. (2020, January 18). $1tn is just the start: Why tech giants could double their market valuations. *The Observer*. https://www.theguardian.com/technology/2020/jan/18/1-trillion-dollars-just-the-start-alphabet-google-tech-giants-double-market-valuation

Posner, E. A., & Weyl, E. G. (2018, April 20). Want Our Personal Data? Pay for It. *Wall Street Journal*. https://www.wsj.com/articles/want-our-personal-data-pay-for-it-1524237577

Siegele, L. (2020, February 20). A deluge of data is giving rise to a new economy. *The Economist*. https://www.economist.com/special-report/2020/02/20/a-deluge-of-data-is-giving-rise-to-a-new-economy

Statista. (2020). *WeChat: Active users worldwide*. Statista. https://www.statista.com/statistics/255778/number-of-active-wechat-messenger-accounts/

The Economist. (2020, February). How to make sense of the latest tech surge. *The Economist*. https://www.economist.com/leaders/2020/02/20/how-to-make-sense-of-the-latest-tech-surge

Wang, Y. (2018, March 28). *Is Alibaba Losing To Tencent In China's Trillion-Dollar Payment War?* Forbes. https://www.forbes.com/sites/ywang/2018/03/28/is-alipay-losing-to-wechat-in-chinas-trillion-dollar-payment-war/

Whitler, K. A. (2019, May 1). What Western Marketers Can Learn from China. *Harvard Business Review*, *May–June 2019*. https://hbr.org/2019/05/what-western-marketers-can-learn-from-china

Wills, J. (2020, April). *7 Ways Amazon Uses Big Data to Stalk You*. Investopedia. https://www.investopedia.com/articles/insights/090716/7-ways-amazon-uses-big-data-stalk-you-amzn.asp