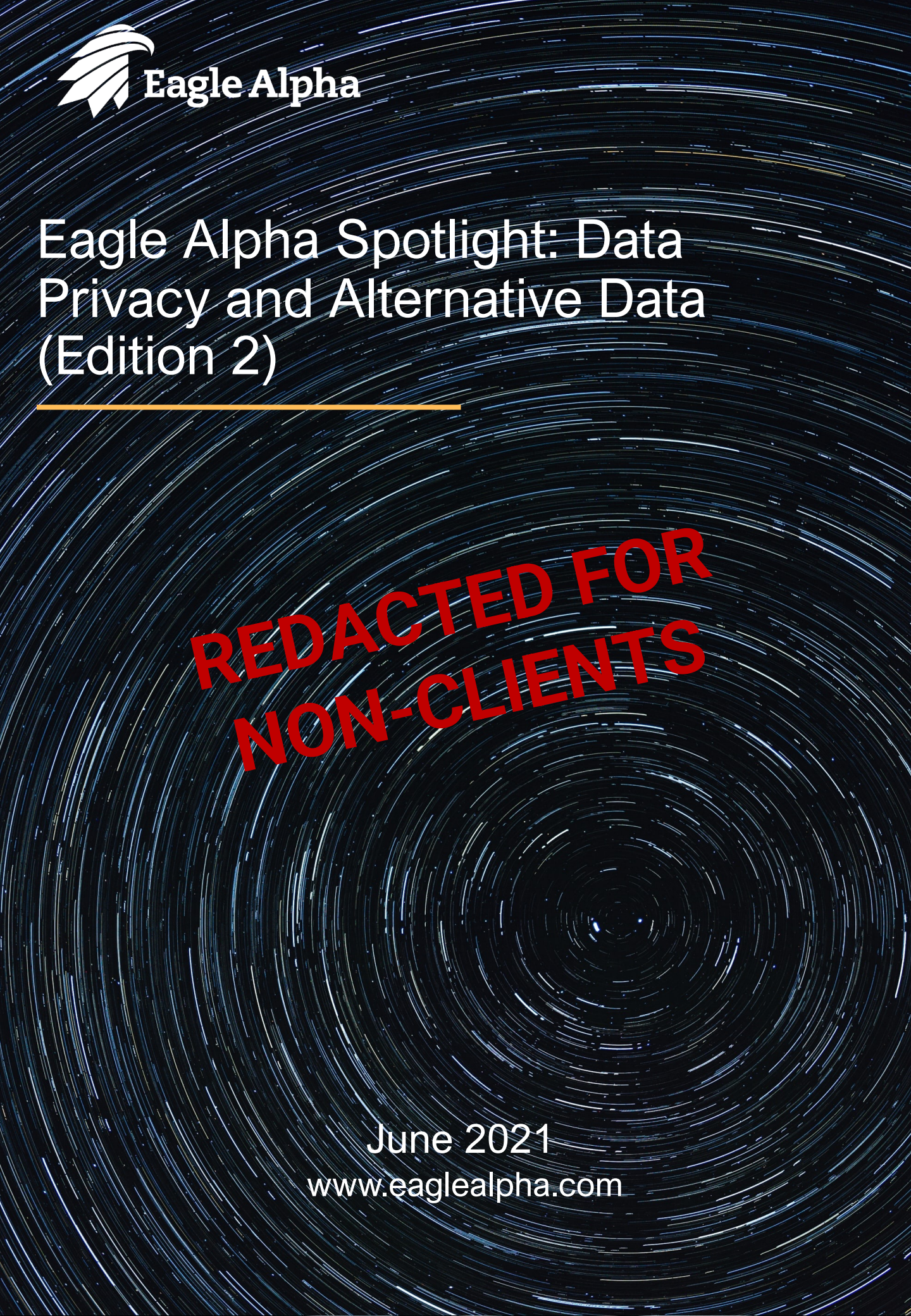


Eagle Alpha Spotlight: Data Privacy and Alternative Data (Edition 2)

REDACTED FOR NON-CLIENTS

June 2021

www.eaglealpha.com

Table Of Contents

Executive Summary

Background

As one of the leaders in the alternative data space, Eagle Alpha makes it a priority to stay up to date with legal and compliance issues across the alternative data landscape. This paper is an exploration into recent data privacy developments and particularly how these developments are impacting the alternative data landscape.

Alternative data sources, specifically datasets harnessing consumer panels, are affected greatly by new regulations and restrictions impacting on how users can be tracked across digital platforms. This has led to numerous legal disputes as well as Big Tech "gatekeepers" implementing updates, in turn forcing firms reliant on these gatekeepers to change their ways. This has resulted in loss of panels for data vendors, with some exiting the market as a result.

The importance of delivering trust and transparency to consumers is now more important than ever, and through the rapid increase in regulations, some companies have begun to market security and consent as a key feature of their service.

GDPR's success in Europe has had a knock-on effect in other regions with an increase of legislative bills passing throughout the U.S. as well as further afield. China is also beginning to make successful strides in how they monitor and control digital misconduct by implementing new regulations across app stores. On one level these changes are to protect the country's digital citizens as well as to promote fair competition, but at a deeper level to protect data from external entities. A common theme coinciding with data privacy is the safe-guarding of data both at a company and country level.

Structure of the Paper

This paper pulls together publicly available data along with insights from vendor interviews and Eagle Alpha's proprietary articles and webinars. Furthermore, the paper also leans heavily on insights from our legal partners, New York law firm Lowenstein Sandler, who are regular contributors to our content.

We have grouped our insights into 5 key sections:

- Major data privacy trends affecting alternative data,
- Data sources in the regulatory spotlight and the legal cases that surround them,
- A section that looks beyond regulation to how companies are self-regulating and restricting the way data is tracked and collected,
- Considerations beyond regulation, such as the developing perceptions of consumers and how "gatekeepers" are impacting data collection and availability.
- An in-depth analysis on important developments being introduced by "gatekeepers" like Apple and Google, and how these changes are impacting the mobile app ecosystem in particular.

Executive Summary

Updates for Edition 2

Edition 2 of this paper considers rapidly developing changes across the alternative data landscape in the first half of 2021. There have been several material updates from edition one:

- Regulations: These include updates surrounding federal law, COPPA, and developments in China related to data collection and distribution.
- Data sources: Recent developments in the alternative data space surrounding mobile app data, web scraping and web traffic data.
- Gatekeepers: We have added a section detailing the changes around data collection instigated by app store gatekeepers Apple and Google. This includes a deep-dive into how Apple's iOS 14.5 update has impacted both app data and location data.

Dallán Ryan
Analyst, Data Strategy
Eagle Alpha

Section 1 – Major Data Privacy Trends Impacting Alternative Data

In this section we explore four major data privacy trends impacting alternative data:
- Changing Consumer Attitudes.
- Data Privacy Regulations.
- Regulation of Big Tech.
- COVID-19.

1.1 Changing Consumer Attitudes

In May 2019, Consumers International and the Internet Society explored consumer views towards the internet of things and discovered that 69% of people surveyed had concerns around how their personal data is collected via mobile apps. The survey also found that only 50% of people were aware of how to disable the collection of their data.[1]

In June 2019, Edelnam, a global PR consultancy, released 'In Brands We Trust', a report exploring consumers' opinions based on brands they interact with.[2] Through this survey, Edelnam discovered that 81% of consumers feel that it is important for them to have an understood trust with a brand before buying from it. This points towards the increasing value for companies today to strive towards a better effort and to act responsibly when it comes to consumer data collection, while remaining trustworthy and transparent, and disclosing how they intend to use the data.

In recent years, privacy concerns have increased due to widespread consumer awareness around the value of user data. Several high-profile news stories, most notably the Cambridge Analytica scandal, have brought data privacy issues to the forefront of mainstream news, causing consumers to question their digital choices more and more. As digital technology continues to evolve, consumer dependence on it also increases.

Consumers have become progressively mindful when sharing data and have grown to understand how companies use the data they collect through mobile apps, websites and other digital channels. Increased regulations and consumer awareness has provided several companies with the idea to use this newly adopted consumer mentality to their advantage by promoting business transparency and data privacy as a key feature of their offerings. One example of this is Apple's giant billboard that was located in Las Vegan promoting product security with the statement reading: "What happens on your iPhone, stays on your iPhone."[3]

In April 2020, McKinsey & Company surveyed 1,000 North American consumers to determine their views surrounding "data collection, hacks and breaches, regulations, communication, and particular industries."[4] The consensus from the findings pointed towards today's consumers becoming more aware of how they share their data and with whom they share it with. Additionally, the lack of trust that was recorded in the findings stemmed from the recent number of high-profile consumer data breaches that have made news headlines over the past number of years.

[1] The trust opportunity: Exploring consumer attitudes to the internet of things, 2019
[2] Edelman trust barometer special report: In brands we trust?, 2019
[3] Apple's iPhone privacy billboard is a clever CES troll but it's also inaccurate, 2019
[4] The consumer-data opportunity and the privacy imperative, 2020

As shown in figure 1, findings from the McKinsey survey pointed towards healthcare and financial services as the most trusted industries for protecting private data, whereas consumer packaged goods, agriculture, oil and gas, and media and entertainment were least trusted.

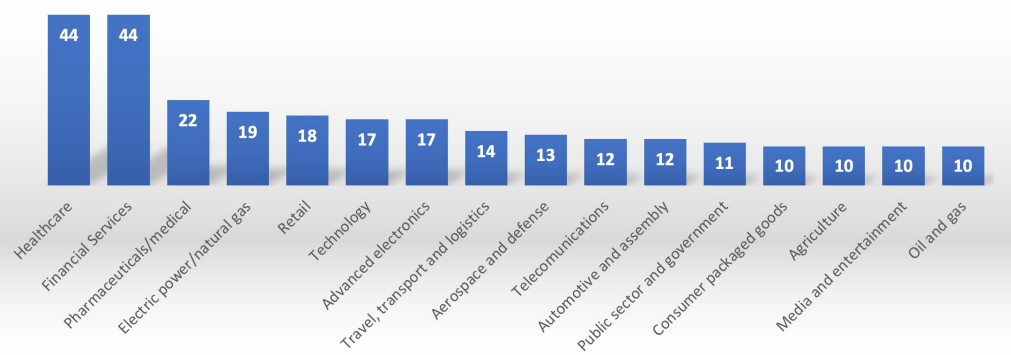


Figure 1: Consumer Opinions of Most Trustworthy Industries (Source: McKinsey Survey of North American Consumers on Data Privacy and Protection, 2019)

Seen in figure 2, an additional study quoted by McKinsey found that two-thirds of consumers surveyed said that it was imperative that the contents of their email, along with the identity of correspondents, should remain private and only accessible to authorized parties. Half of the consumer panel surveyed answered that they were more likely to trust companies that asked for information related only to its product or limited the amount of information it asked for. Additionally, half of the respondents agreed that they were more likely to trust a company that reacts quickly to data breaches.

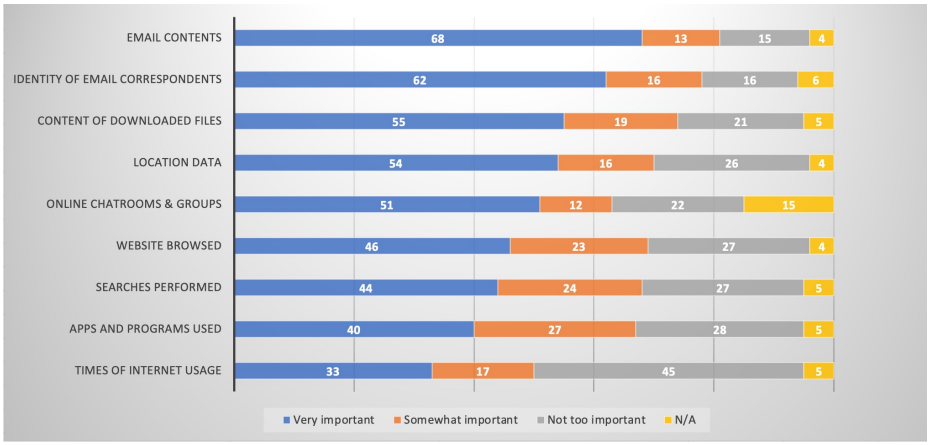


Figure 2: Consumer Privacy and Protection Concerns by Type of Digital Data (Source: Internet & American Life Project, Pew Research Center)

The information collected in both studies points towards the growing consumer awareness and confirms the needs for companies to listen to consumer needs around privacy, security and transparency.

1.2 Data Privacy Regulations

The General Data Protection Regulation, or GDPR, was drafted and passed by the European Union (EU) and put into effect in May 2018. It is the toughest privacy and security law in the world, with the power to implement harsh fines for violations stretching to 20 million euro or 4% of global revenue (whichever is higher).[5]

While there is currently nothing close to GDPR in the United States, frustrating legal and compliance professionals across the country,[6] the California Consumer Privacy Act (CCPA) offers residents of California a degree of protection that is seen in the EU's GDPR legislation.[7] Under the CCPA, consumers have the right to know what personal information is collected, the right to delete their collected personal information, the right to opt-out of the sale of personal information, and the right to non-discrimination for exercising their CCPA rights.

After the success of the CCPA, several other states followed suit developing and implementing their adapted legislation around the use of data security and privacy for the online consumer.[8] One of these states being Virginia, who on the 5th February 2021 approved the Consumer Data Protection Act (CDPA), a framework for controlling and processing personal data of Virginia residents. This act is set to become effective on January 1st, 2023.[9] Additionally, there are several states with ongoing developments to establish data protection laws. The CCPA has proved to be the baseline regulation in the U.S. that companies must follow from a legal perspective, even though it might not be enforced in the state they reside in.

Two weeks after Virginia approved the CDPA, the Information Transparency and Personal Data Control Act was introduced into the 117th US Congress.[10] This act, the first comprehensive privacy legislation to appear in front of this congress, aims to create protections around the collection, processing and sharing of sensitive personal information and non-sensitive information, where companies would be required to allow consumers to opt out of data collection at any time.

This development provides some insight into a future federal law, however, in June 2021, Peter Greene of Lowenstein Sandler felt that although buyside consumers of alternative data have been waiting for federal privacy legislation to replace the patchwork of state laws, we probably won't see this progress until late 2021-22.[11] Now that we are in 2021 it seems very likely it will be 2022 or beyond before we see any developments.

With the change in presidential administration in the US, a new FTC chair has been appointed. Lina Khan, known to be a fierce advocate of data privacy and antitrust enforcement against the Big Tech, is expected to investigate how data collection is contributing to the dominance of U.S. tech giants.[12] Lina Khan is also expected to inherit the rulemaking initiative that was started by acting chair, Rebecca Kelly Slaughter, before Khan's appointment.

[5] What is GDPR, the EU's new data protection law, 2021
[6] Federal privacy legislation & settlement of the weather channel case, 2020
[7] California consumer privacy act (CCPA), 2021
[8] The evolving data privacy landscape: GDPR, CCPA and similar data protection laws, 2020
[9] Will Virginia be the second state to enact major legislation?, 2021
[10] New federal bill introduced – could 2021 be the year?, 2021
[11] Quarterly wrap with Lowenstein Sandler (Q2 2021), 2021
[12] Lina Khan bring scrutiny to Big Tech data dominance as FTC chair, 2021

Included as part of this agency-wide rulemaking initiative is an update to the Children's Online Privacy Protection Rule ("COPPA") which was first published by the FTC in 1998.[13] COPPA implements certain requirements for websites and online services that collect information from children under the age of 13. Since then, the FTC have expanded the rule alongside increased data collection, rapidly changing technology and new techniques used. From the 2013 update, this includes geolocation data, identifiers that can be used to track user behaviour, photos, videos and audio files. COPPA places the responsibility to gain parental consent on the data collector.

Although this rule has been difficult to enforce in the past, the FTC recently updated its FAQs surrounding COPPA and outlined that without verifiable consent, it could leave data collectors that do not comply, vulnerable. In March 2021, before the appointment of Lina Khan, acting FTC chair Rebecca Kelly Slaughter stated that the FTC may "increase civil investigations, enforcement and penalties for violations of its Children's Online Privacy Protection Act Rule".[14]

The movement of data between Europe and the US has also been a topic for interesting discussion. The US Privacy Shield Framework was agreed upon by the EU in July 2016, and by Switzerland in January 2017.[15] The goal of the shield was to provide a framework to help companies comply with data protection requirements when transferring personal data from the EU and Switzerland to the US.

As of July 16, 2020, the Court of Justice of the European Union declared the Privacy Shield to be an inadequate mechanism for protection of data transferred between the EU and US.[16] While the Privacy Shield is no longer a valid mechanism for the process of transferring personal data, the companies involved are still obligated to continue meeting commitments, with failure to comply resulting in enforcement by the Federal Trade Commission (FTC). From conversations with data vendors, we have been told that data transfer between the EU and the US is still possible, however, it has become much more difficult and now requires a lot of paperwork.

If we consider regions outside of the US and Europe, there have also been major developments in China and India. There are over 3.5 million active apps in China and this number is growing daily,[17] putting huge pressure on the Chinese government to enforce stricter regulation. The swift evolution of mobile apps has brought about a rapid increase in data privacy risks and also additional risks concerning leakage of personally identifiable information (PII). With users sharing information openly across platforms and web cookies tracking every click, the vast amount of data that is stored is hugely valuable and at risk data breach.

Chinese consumers have become increasingly aware of how their data is being used and are now complaining to the relevant data authorities over abuse of personal data. Because of this, regulators are beginning to improve their supervision against these firms, especially how they use their customers' PII.[18]

[13] Children's Online Privacy Protection Rule ("COPPA"), 2021
[14] FTC signals increased enforcement for COPPA violations, 2021
[15] Privacy shield overview, 2021
[16] The EU-US Privacy Shield struck down by the European Court of Justice , 2020
[17] Mobile apps in China - statistics & facts, 2020
[18] China removes 94 mobile apps for privacy violations, 2020

On the 27th November 2020, China's Ministry of Industry and Information Technology announced that it had completed an assessment of 440,000 mobile apps. From this investigation they flagged 1,336 apps that indicated minor privacy violations that could be resolved, but found that 94 apps had severe violations and were removed from the app store. Coming into 2021, China's ministry had announced plans to investigate 1.8 million apps using AI and big data methods, and had formulated 11 standards for app company data collection.

In February 2021, Marissa Dong of Jun He Law Offices in Beijing provided Eagle Alpha clients with an update on the rapidly developing regulations in China.[19] In her words, information technology-related legislation has been developed very quickly, and fast-tracked legislations around the Personal Information Protection Law and Data Security Law are at the forefront of these developments.

The Civil Code of the People's Republic of China came into force on January 1st, 2021, outlining definitions, requirements, civil liabilities, and individual rights with respect to data privacy and personal information. Also included was 53 national standards and 64 different research promulgations with respect to cyber security and data privacy and protection by the China National Information Security Standardization Technology Committee, also referred to as TC260.

The Chinese government have also targeted specific alternative data sources like app data, consumer transaction data, web-scraped data and geolocation data. Concerning these sources, the governing bodies have laid out guidelines around the over-collection of data, what China considers 'important data', anti-crawling measures, and in-app consent. For data buyers in the US or Europe wanting to acquire data from China, it is important to seek local counsel before purchase as regulations in the region are changing quickly.

Outside of China, the Personal Data Protection Bill (PDPB) was introduced by Indian Parliament in December 2019 and was being analysed by a Joint Parliamentary Committee as of March 2020. This new data legislation is set to be the most comprehensive data protection bill in the world, borrowing concepts from GDPR, including data collection and processing, consent, deletion of data, and addresses de-identified personal data and encryption.[20] Almost all businesses across the Indian economy will have to meet the conditions of the bill, including e-commerce, social media, and IT companies, but also non-internet related businesses including real-estate, hospitals, pharmaceutical companies and brick-and-mortar stores.

1.3 Regulation of Big Tech

In recent times, US Big Tech (Facebook, Apple, Google and Amazon), with a combined market value of more than $5 trillion,[21] has dominated the information technology space. This dominance has been the driving force of new legislation on data processing and handling practices. The four largest tech giants are branded as "gatekeepers" to their respective industries where they control prices and distribution of goods and services, forcing the hands of third parties using their platforms.

[19] Legal considerations in China, 2021
[20] Data protection bill in India: Potential implications for alternative data ecosystem, 2020
[21] House lawmakers condemn Big Tech's 'monopoly power' and urge their breakups , 2020

Following a 2020 report led by House of Representatives lawmakers in Washington, Google and Amazon received the most attention, with Apple and Facebook also having sections dedicated to them.[22] Google holds a monopoly in search and search advertising and was found to have used anticompetitive tactics to improve the quality of its features.[23] Amazon, on the other hand, spanned across several industries and used its e-commerce platform to compete unfairly against merchants by promoting their brand ahead of third parties.[24] 2.3 million third-party sellers are active on Amazon's marketplace, with 37% of these relying on it as their sole source of income.[25] Facebook has a monopoly over social media, acquires companies like Instagram and WhatsApp or copies competitor features to maintain power. Apple has monopoly power over the app's marketplace for iPhones and iPads, with app developers forced to go through the app store where Apple takes up to 30% of app sales.

In 2019, the FTC fined Facebook $5 billion for privacy violations and YouTube $170 million for collecting children's personally identifiable information without parents' consent.[26] As of December 2020, the FTC ordered Facebook, Twitter, Amazon, TikTok's ByteDance, as well as several other social media companies, to provide detailed information on how they collect data and use consumer PII. US law firm and Eagle Alpha partner, Lowenstein Sandler has said, "The federal government's continuing interest in data collection, data use and anonymization are important to the hedge fund community as the consumer's permission for his/her data to be used is at the centre of the data provenance analysis funds must conduct before they purchase any type of alternative data."

Furthermore, the EU has suggested a plan to control monopolisation of Big Tech by introducing legislation and outlined that companies "shall not use data collected from the platform...for [their] own commercial activities...unless they [make it] accessible to business users in the same commercial activities." The Digital Services Act (DSA) is due to come to fruition in late-2021 and aims to restrict big technology companies from monopolising the data market while also creating a benchmark for global digital practices across competition, tax compliance and illegal content.

In China, as mentioned previously, data privacy regulations are moving quickly. China's Big Tech companies known as BAT – Baidu, Alibaba and Tencent – have all come under fire for different abuses under Chinese legislation. Most recently Ant Group, an affiliate company of Alibaba Group, had their planned $35.5 billion IPO suspended, while Alibaba was fined $2.8 billion due to anti-trust violations. With China promising that regulation of Big Tech is part of its plan to become a tech superpower, the mandates include stricter compliance for global listings, limits on information monopolies and transparency on data gathering.[27]

The regulation of Big Tech is forcing these "gatekeepers" to change the amount of data and types of data that they and their partners are collecting, as well as the techniques they are using to collect this data. We discuss this in more detail in Section 4.

[22] The house antitrust report on big tech, 2020
[23] Google abuses its monopoly power over search, justice department says in lawsuit, 2020
[24] Amazon is the target of a small-business antitrust campaign, 2021
[25] US antitrust probe finds 'alarming pattern' of innovation-stifling practices, 2020
[26] FTC has ordered Big Tech to provide detailed information on how they collect and use data, 2020
[27] Legal considerations in China, 2021

1.4 Covid-19

On 11th March 2020, the World Health Organisation (WHO) announced Covid-19 as a global pandemic. Big data, artificial intelligence and blockchain technology have been central to understanding and reacting effectively to the virus.[28] Location data collected from mobile devices has helped governments and private corporations understand movement patterns and provide insights into the spread of the virus. Blockchain has provided an opportunity to use technology to control a secure cryptographically maintained database of stocks and medication for supply chain efficiency in healthcare, while video-based classrooms such as Zoom and virtual reality (VR) technology have offered new ways for education delivery. These advances in previously underutilised technology due to Covid-19 also introduce new challenges in dealing with the increased digital footprint and risk of data security issues. The Covid-19 crisis has required companies and governments to rethink the way they operate, and has proven to be the first real obstacle that GDPR has had to overcome since it came into force.[29]

Companies such as TripleBlind and University of California, San Francisco (UCSF) spinout, Syntegra, have been using their security-focused technology to benefit processes throughout the pandemic. TripleBlind is a privacy-as-a-service (PaaS) company offering privacy-focused solutions based on advanced mathematics. In late 2020, it announced a collaboration with the Mayo Clinic to develop a next-generation algorithm for sharing and training on encrypted data.[30] Additionally, Syntegra has developed an algorithm for healthcare systems to create synthetic data by stripping names, addresses and other information protected by healthcare privacy laws, allowing researchers access to data by creating artificial people and protecting the privacy of the real patient.[31]

[28] Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection, 2020
[29] Privacy and data protection in the age of COVID-19, 2020
[30] TripleBlind collaborates with Mayo Clinic on next generation algorithm sharing and training on encrypted data , 2020
[31] How a UCSF spinout is turning private Covid patient data into tools for researchers , 2020

Section 2 – Data Sources in the Legal & Regulatory Spotlight

This section discusses the alternative data sources that have gained the most attention from legal and regulatory bodies, or have incurred negative coverage in mainstream media, and as a results are at risk of attracting the attention of regulators. The categories discussed in this section are:

- Geolocation data.
- Consumer transaction data.
- Consumer credit data.

2.1 Geolocation Data

In December 2018, the New York Times published an article outlining the vast amount of data gathered via mobile devices, and how data collectors then offer this data for up for sale.[32] Knowledge surrounding geolocation data is becoming increasingly mainstream with users aware that advertisers, retailers and hedge funds are using their personal data to improve marketing campaigns, products and to develop investment strategies. According to the New York Times, sales of location-targeted data reached an estimated $21 billion in 2018.

The Weather Channel App is the most popular mobile weather app in the United States, with over 50 million users. In 2019, the city of Los Angeles filed litigation against The Weather Channel App, a company owned by IBM Corporation, alleging that the app misled millions of people into granting access to their location data for sale to third parties. IBM had called this accusation 'baseless', but came to a settlement with the city of LA.[33]

The settlement required the app owner, IBM, and the app's operator, TWC Product and Technology LLC, to improve transparency by updating the location-tracking consent screens. As part of the settlement, the app owner and app's operators are legally required to inform the city of Los Angeles of any changes to the consent screen for two years following the settlement.

2.2 Consumer Transaction Data

In January 2020, US lawmakers wrote a letter to the FTC calling for an investigation to be made into Yodlee and its parent company Envestnet. They alleged that the company's sale of US consumer data violates FTC regulations. Similar to Los Angeles versus The Weather Channel App, the lawmakers claim that Envestnet does not clearly inform consumers that their data will be sold to third parties. Envestnet responded to the accusations by saying that they complied with all data collection laws and per industry best practices.[34]

[32] Your apps know where you were last night, and they're not keeping it a secret, 2018
[33] Los Angeles settles Weather Channel lawsuit, lets it keep selling location data to advertisers, 2020
[34] Envestnet and Yodlee face class action lawsuit, 2020

On August 25th, 2020, Yodlee and Envestnet were both subject to a class-action suit alleging that their data collection practices do not obtain consent from users for the data that is sold. The suit claimed that companies using Yodlee software, like PayPal and Bank of America, had failed to take the required steps to protect user data.

Lowenstein Sandler commented on this by saying, "from an alternative data perspective, this class action highlights the continuing intersection amongst privacy, PII and securities laws concerns. As class action lawyers and politicians continue to criticize the collection and repackaging of consumer data, especially financial transaction data, fund managers must be ever careful to diligence the provenance of the data collected by suppliers of alternative data."

2.3 Consumer Credit

In October 2020, the Information Commissioner's Office (ICO) published a report on Experian, a credit reference agency, after it was found that they were in breach of data protection laws by trading, enriching and enhancing users' data without their knowledge.[35] This breach was first flagged in 2018 by campaign group Privacy International, and the ICO spent two years investigating the firm. The ICO have ordered Experian to make radical adjustments to how they handle personal data within its direct marketing services by July 2021, or it could face a £20m fine, or 4% of their global annual revenue. The report outlined that the data collected by Experian had been traded by three firms, including TransUnion and Equifax.

The investigation into the credit rating agencies, or CRAs, found that 'invisible processing' was taking place. This is when personal data is obtained from somewhere other than directly from the individual and without their consent. This "invisible" processing resulted in products that were being used by political parties, corporates and charities. These organisations used the data to find new customers, source people most likely to be able to afford certain goods and services and to contribute to building consumer profiles.

With companies becoming increasingly remote-based throughout 2020, CRAs and similar companies with access to huge amounts of personal data became more at risk of breaching GDPR legislation unknowingly. Britt Endermann, Forensic Risk Alliance's (FRA) Chief Technology Officer said, 'This problem is far more widespread than anyone would know right now, from very large companies to the smaller and midsize companies.'

Lowenstein Sandler also added, "This is a further example of the need for hedge fund managers who consume alternative data to investigate whether the data vendor has the express right to sell the personal transaction data to funds for use in financial services. This applies to credit card and other transaction data."[36]

[35] ICO takes enforcement action against Experian after data broking investigation, 2020
[36] The Information Commissioner's Office takes action against Experian, 2020

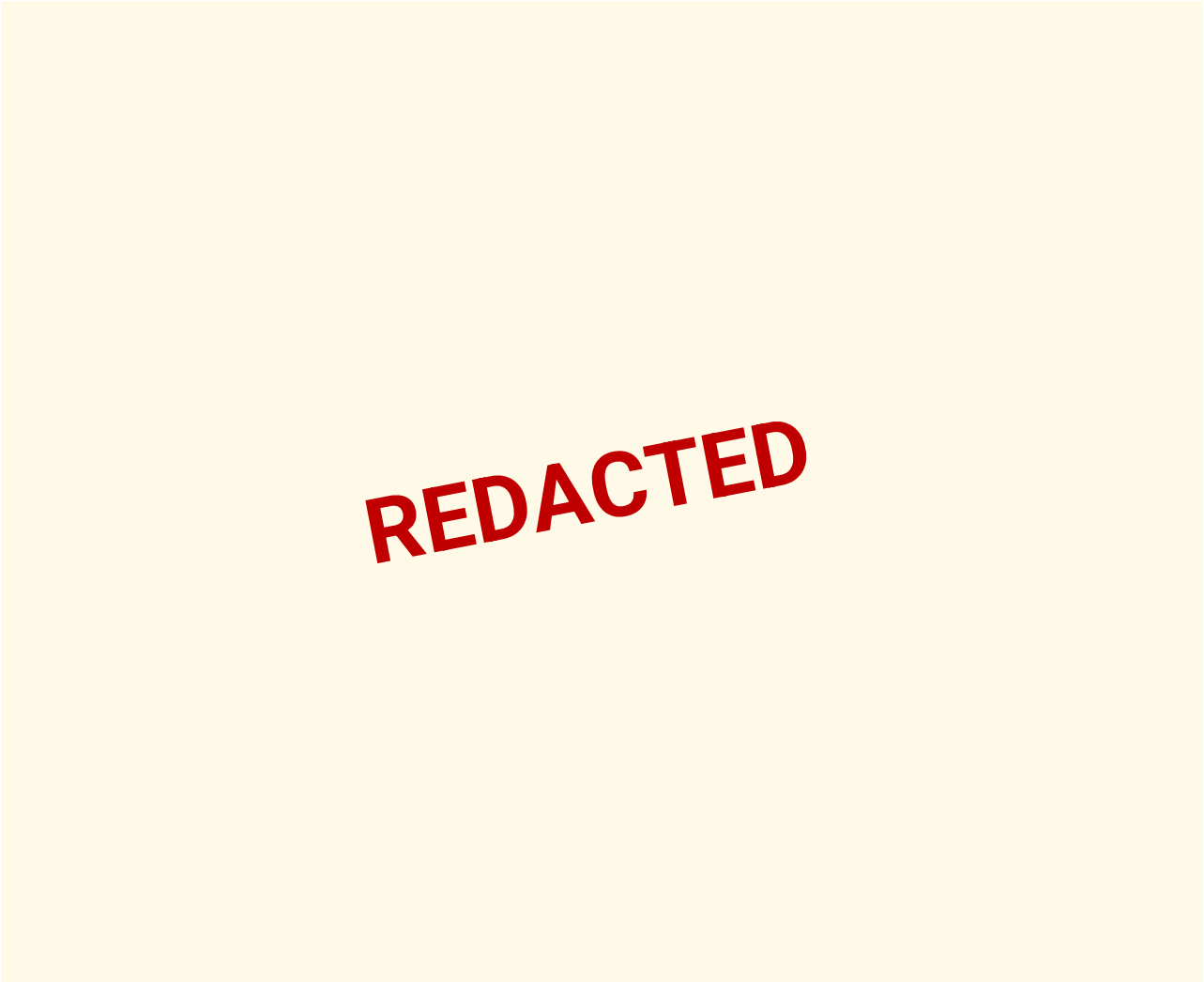
Section 3 – Beyond Regulations

Legal and regulatory actions are clearly a major concern for players in the data ecosystem, however, there are factors beyond regulations that are also impacting the alternative data space. This section discusses the alternative data sources that have been impacted by forces outside of regulations, including Big Tech "gatekeepers" and changing consumer perceptions. In our conversations with data vendors on the topic of data privacy, it was apparent that the actions of Big Tech and the data "gatekeepers" are a bigger concern for the industry than regulators.

The categories discussed are:

- App data.
- Web-scraped data.
- Web-traffic data.
- Email receipt data.
- Social media data.

3.1 App Data



REDACTED

In June 2021, we published a paper as part of the Eagle Alpha Spotlight series where we explored mobile app data and the opportunities and challenges associated with it. In this paper we also spoke directly to the app data vendors and provided a breakdown of their data offerings for buyers. You can access this paper here.

3.2 Web Scraping

REDACTED

3.3 Web-Traffic

REDACTED

REDACTED

3.4 Email Receipt Data

REDACTED

3.5 Social Media Data

REDACTED

Section 4 – Tightening Data Privacy at Apple and Google

4.1 Apple iOS14.5

REDACTED

4.2 Apple's Definition of 'Tracking'

REDACTED

Table 1: Apple's Definition of Tracking (Source: Apple)

4.3 Privacy Labels

REDACTED

4.4 Google's Response

REDACTED

4.5 Impact on Alternative Data

REDACTED

Figure 3: Worldwide Daily Opt-in Rate After iOS 14.5 Launch Across All Apps (Source: Flurry)

Figure 4: US Daily Opt-in Rate After iOS 14.5 Launch Across All Apps (Source: Flurry)

Figure 5: Consumer Panel Decline in Monthly Active Users (Source: Major App Data Provider)

REDACTED

Location Data:

REDACTED

REDACTED

4.6 iOS 15 and Beyond

REDACTED

Conclusion

The ongoing changes across the digital landscape means that the definitions for buzzwords like user tracking and data privacy is in a constant state of development. At present, we understand what both regulators and big tech gatekeepers consider to be legal and also in breach of a company's terms of service, but these can change quite quickly. As mentioned previously, vendors are most focused on developments surrounding Big Tech as they can update and change requirements overnight.

Sitting alongside changes to both regulations and companies are consumer perceptions, which have changed dramatically over the past decade. Consumers are very much aware of the value of their data and are now being offered the choice as to what data they allow to share. Facebook's infamous motto is to "move fast and break stuff." While it is important to move fast, breaking the trust of consumers is something that will contribute to swift self-destruction of companies over-collecting or acting in nefarious ways.

Finally, for buyers of data, data provenance and the reliability of the data source, is increasingly important. This is particularly true for the investment industry as data provenance is a core protection against claims of MNPI. Data buyers must also look beyond the immediate legal and regulatory requirements to consider potential changes to regulations, the potential for increased self-regulation from Big Tech and the changing consumer attitudes towards data privacy. If a firm fails to do this, then external datasets that are considered valuable may not be as accessible as once thought or worse, a company could find themselves on the wrong side of a regulatory investigation or media storm.

[62] Apple - Outstanding new privacy feature will change your iPhone forever, 2021

Select Further Reading From Eagle Alpha

Alpha Centre

- Eagle Alpha Spotlight - Environmental Data
- Eagle Alpha Spotlight - Mobile App Data
- Advanced Alpha Testing Techniques
- 2021 INTERACT Conference Wrap
- External Data for Retail Success
- A Comparison of Major Consumer Transaction Vendors for Product Level Analysis

Strategy Centre

- Implementing a Data Strategy in Private Markets
- Eagle Alpha's Buyside Alternative Data Survey 2021
- Strategy Workshop with Matthew Ekroth
- How Leading Quant Funds Use Alternative Data

Legal & Compliance

- Quarterly Wrap with Lowenstein Sandler (Q2 2021)
- SEC's 2021 Focus on Alternative Data
- Facebook's Response to Web Scraping
- Europe Focus with Ashurst LLP
- Quarterly Compliance with Davidson Kempner
- Quarterly Wrap with Lowenstein Sandler
- Legal Considerations in China

Expert Hub

- Machine Learning Fails When We Need It Most
- Accelerating Data Onboarding - What Progress Have We Made This Year?
- Mapping Datasets to Symbols
- Do Trade Creditors Possess Private Information? Evidence from Firm Performance
- Incorporating Alternative Data Into Fundamental Processes

About Us

Established in 2012, Eagle Alpha is the pioneer connecting the universe of alternative data. We are the leading alternative data aggregation platform with supporting advisory services for data buyers and data vendors.

First adopted by alpha-seeking hedge funds over 10 years ago, alternative data is now being sought for use in the wider asset management space, as well as the private equity and corporate verticals.

Eagle Alpha was one of the first companies to recognize the value from these new data sources and has been investing in educating and connecting alternative data vendors and buyers since 2012, in the process building trusted relationships with both sides of this market.

As of May 2021, Eagle Alpha has profiled in excess of 1,500 datasets and provides annual solutions to data buyers and data vendors globally.

A unique breadth of datasets, knowledge of the industry and client relationships have cemented Eagle Alpha as the global leader and strategic partner in the data space.

Eagle Alpha partners with industry leaders to continue to shape the industry:

1. J.P. Morgan, lead sponsor of our data conferences.
2. FISD, member of this association to create standards for the industry.
3. Lowenstein Sandler, partner with this US law firm.

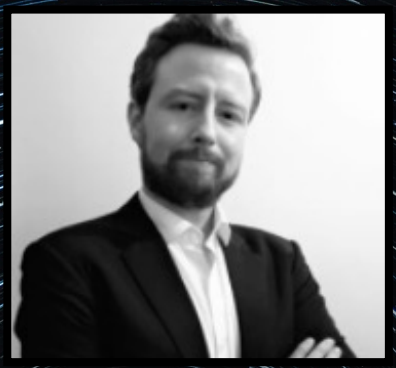
Eagle Alpha

CONTACT US:

USA: +1 646 843 6048
UK: +44 (0) 20 7151 4880
Email:
datastrategy@eaglealpha.com

Dallán Ryan
Analyst, Data Strategy
Dallan.Ryan@eaglealpha.com

Dallán supports research and content goals for the Data Strategy solution Eagle Alpha. Dallán's experience also spans business development and digital marketing for technology-led startup companies.



Ronan Crosson
Director, Data Strategy and Analytics
ronan.crosson@eaglealpha.com

Ronan manages Eagle Alpha's analyst team and is responsible for the Data Strategy solution. Ronan's experience spans the front office and middle office on the buyside as well as building and managing data science and analyst teams at Eagle Alpha.