Docket No. CFPB 2021-0017

Comment on

An Inquiry into Big Tech Payment Platforms

Steve Perkins
Ann Baddour

December 2021

Executive summary

We recommend that the CFPB require that payment platforms follow the Fair Information Practice Principles. Three principles apply directly to harvesting and monetizing user data. **Companies should apply these principles and be prohibited from limiting user access to services if a user chooses to protect personal data:**

- **Collection Limitation Principle –**
  - **Ask** user permission to gather their personal data
  - **Limit** collection to the data needed for a transaction
- **Purpose Specification Principle -**
  - **Specify** the purposes for which their data will be collected
  - **Use** data only for the fulfillment of those purposes
- **Use Limitation Principle –**
  - **Ask** permission to use data for purposes other than those specified
  - **Ask** permission to sell, disclose, or share user data

An Inquiry into Big Tech Payment Platforms

- The CFPB has ordered six technology platforms offering payment services to turn over information about their products, plans and practices when it comes to payments. Orders were issued to:
  - **Google**
  - **Apple**
  - **Facebook**
  - **Amazon**
  - **Square**
  - **PayPal**

- The information will help the CFPB better understand how these firms use personal payments data and manage data access to users so the Bureau can ensure adequate consumer protection.

https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-tech-giants-to-turn-over-information-on-their-payment-system-plans/

Our comment focuses on two sections of the orders

- Section B: Data Harvesting
  - The Bureau is seeking information about the **data that COMPANY collects and retains as a result of consumers' use of PRODUCT**. The Bureau further seeks to understand the **kinds of data that COMPANY generates from this product use data**—for example, through combining it with externally-sourced data or with other data obtained from the COMPANY's own operations or with data from both such sources. More generally, the Bureau seeks to **understand the purposes associated with the harvesting of different data fields**.

- Section C: Data Use and Monetization
  - The Bureau is seeking information on **how COMPANY monetizes the Product Data described above** – including by improving service delivery to customers of the PRODUCT, **by selling the data directly, and by selling advertising or other targeted content based on attributes derived from the data.**

https://files.consumerfinance.gov/f/documents/cfpb_section-1022_generic-order_2021-10.pdf

The CFPB outlines data harvesting & monetization

- Section B: Data Harvesting
  - The CFPB differentiates between two types of data:
    - Direct – data collected as a result of consumer use of the payment product
    - Indirect – other data the company collects and maintains such as:
      - Data generated or derived from direct data,
      - Internally collected company data on consumers,
      - Externally sourced data about consumers

- Section C: Data Use and Monetization
  - The CFPB lays out three ways companies monetize their harvested data
    - Developing, selling, or marketing products
    - Sharing, selling, disclosing data to 3rd parties
    - Selling advertising based on consumer attributes derived from data

Example of harvesting data

Direct data from use of the product by a consumer for a transaction

Indirect data collected internally on consumers such as use over time, browser info, demos, survey data

Indirect data acquired from external third parties such as data brokers or credit reporting agencies

Indirect data derived from analyzing or manipulating any of the above direct or indirect data

Example of monetizing data

PayPal

Direct data from use of the product by a consumer for a transaction

Indirect data collected internally on consumers such as use over time, browser info, demos, survey data

acxiom TransUnion

Indirect data acquired from external third parties such as data brokers or credit reporting agencies

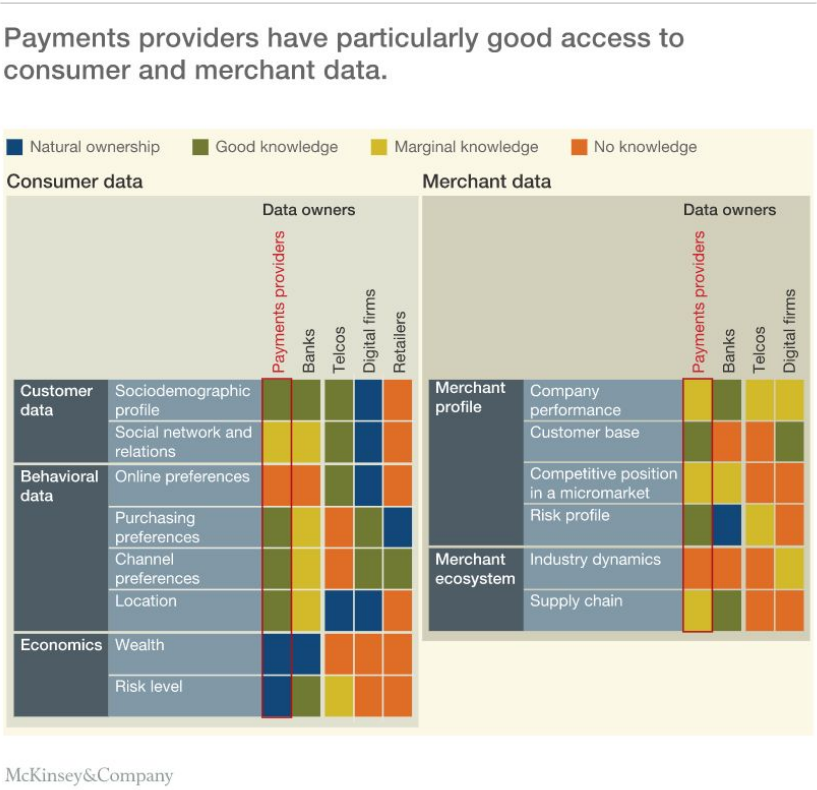
sas FICO

Indirect data derived from analyzing or manipulating any of the above direct or indirect data

Monetize harvested data by:

- **Developing** new products to address unmet consumer needs
- **Marketing** across product lines, cross-selling additional products
- **Selling** data or analysis results to 3rd party brokers
- **Sharing** access to user data with business partners
- **Selling** user attributes to purchasers of advertising to target consumers

"Monetizing data: A new source of value in payments"



As a 2017 McKinsey report says:

- …"**today's payments providers have a treasure trove of data at their fingertips**. By using it to generate insights into consumer purchasing behavior, and coupling these insights with an understanding of emerging macro trends, payments firms can provide better service to customers"
- "But they can also **go a step further by capturing emerging opportunities to extract value through the monetization of the data itself**, either internally or through third parties."

https://www.mckinsey.com/industries/financial-services/our-insights/monetizing-data-a-new-source-of-value-in-payments

Companies often share access to user data with partners

A sample of companies with which PayPal shares user data:

Payment processors (Bank of America, Wells Fargo, American Express, JPMorgan Chase, India's Chargebee, Russia's VTB24, Pakistan's Bank Alfalah Ltd., and others)

Auditors (PricewaterhouseCoopers, KPMG and others)

Credit and fraud agencies (Experian, Equifax, Russia's National Credit Bureau, Cyprus' Au10tix and others)

Financial product providers (such as Santander UK, Deloitte, France's La Poste, BNP Paribas, and others)

Commercial partners (Stubhub, Apple, DHL, UK's Royal Mail, Bulgaria's TELUS, Facebook, and others)

Marketers and publicists (such as Salesforce, Edelman PR, LinkedIn, Google, Poland's Clue PR, Google, Pandora)

Operational service providers (Mailchimp, eBay Enterprise, Amazon Web Services, Salesforce, Google, and others)

Other commercial partners (such as several eBay units, Korea's M3 Mobile, Ireland's Kijiji International and Epinions)

Legal entities (Altep, Consilio, eTERA, Avansic, Deloitte Touche Tohmatsu Ltd., Superior Review and others)

Government agencies (such as the European Consumer Centre Network, various data protection agencies in Europe)

PayPal's own internal units

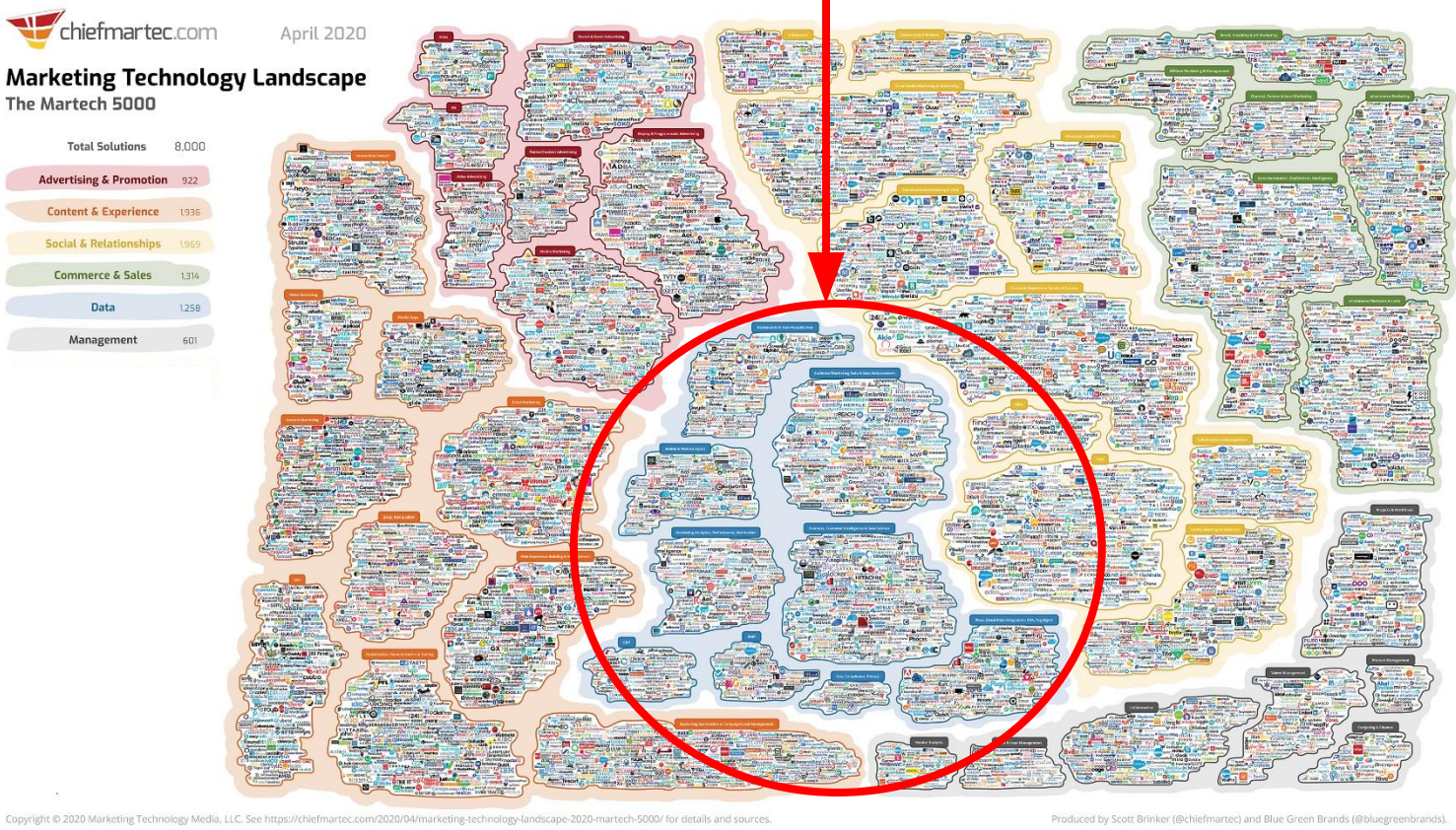
- Some companies say they do not "sell" data. But they do "share" data with partners.
- PayPal, for example, shares user data including:
  - name
  - address
  - phone number
  - date of birth
  - IP address
  - bank account information
  - recent purchases

https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list

https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/

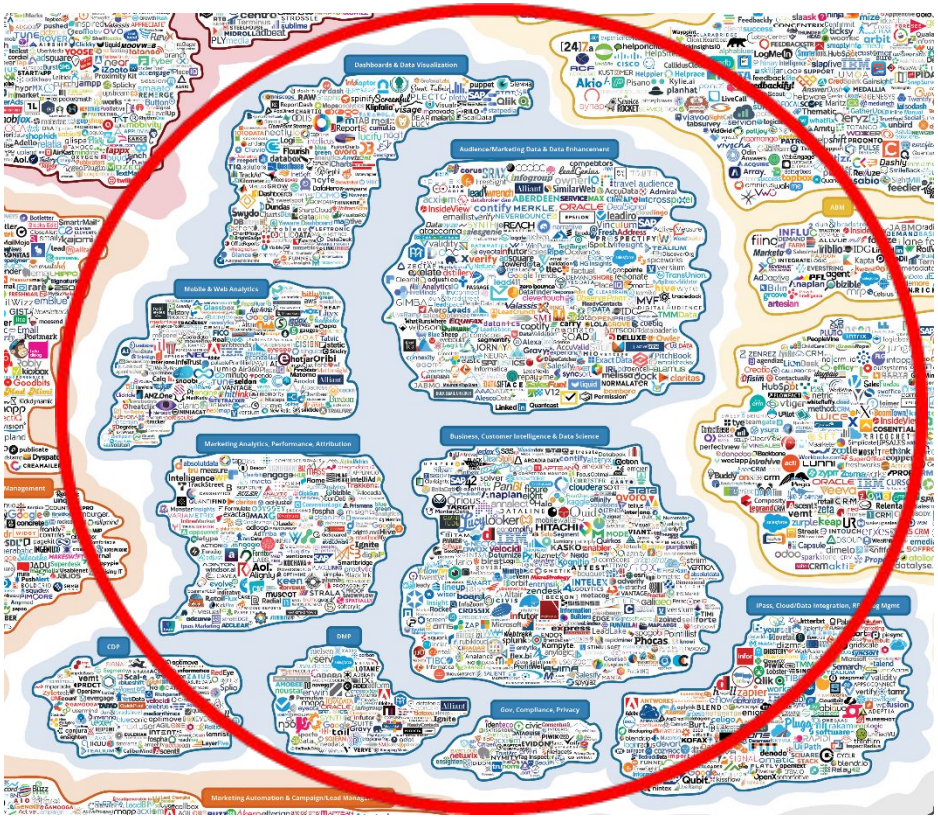
Companies buy indirect user data from third parties

Over 8000 “martech” (marketing technology) companies in 2020
With over 1250 of those selling data and analytical services



https://chiefmartec.com/2020/04/marketing-technology-landscape-2020-martech-5000/

“Data” is the fastest growing martech category



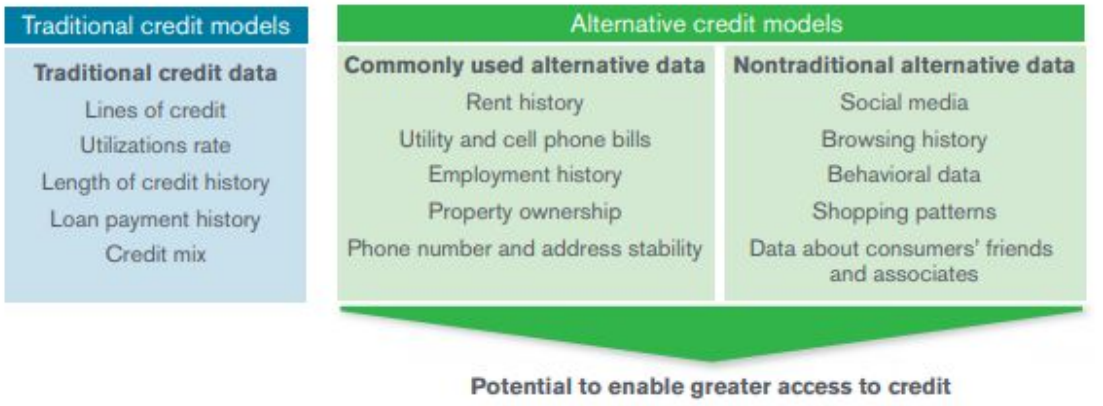
- Payment platforms buy data and analytical services such as
  - Marketing data
  - Data enhancement
  - Customer intelligence
  - Data science
  - Marketing analytics
  - Web analytics
  - Dashboards
  - Data visualization
  - Customer data platforms
  - Data management platforms
- And payment platforms may also sell customer data to martech companies or monetize customer data through enabling targeted advertising by third-parties.

https://chiefmartec.com/2020/04/marketing-technology-landscape-2020-martech-5000/

Companies may also purchase "alternative data"

- Companies typically use **"traditional credit data"** such as loan payment history to assess consumer financial strength.
- But now financial companies may also acquire **"alternative data"** such as address stability, social media, browsing history, and data about friends and associates.

Figure 22: Types of Credit Data

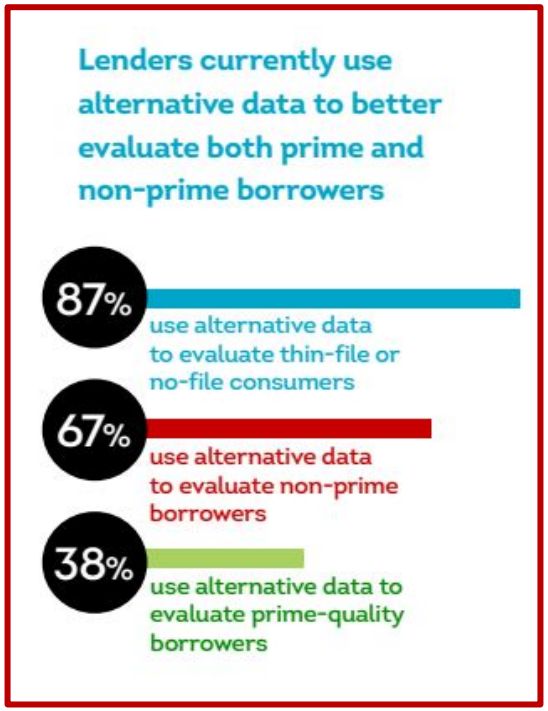


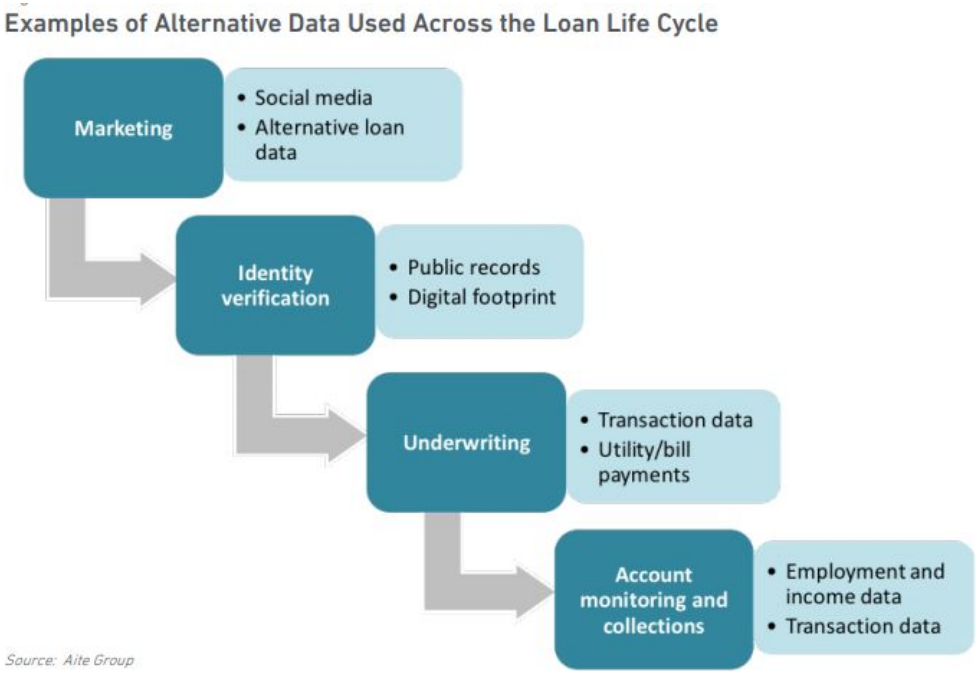
The validity of using nontraditional alternative data in financial services is not known – data could be incorrect and biased.

https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf

Use of alternative data varies by creditworthiness

- Companies often use nontraditional financial data with non-prime customers, but less commonly with prime-quality borrowers.
- Do non-prime customers experience "data abuse" including racial bias, civil rights, and economic exclusion when companies use alternative data?





https://www.experian.com/assets/consumer-information/reports/Experian_Aite_AltDataReport_Final_120418.pdf

https://www.transunion.com/resources/transunion/doc/insights/research-reports/research-report-state-of-alternative-data.pdf

In brief –

Payment platforms harvest direct and indirect data and make money by using it within the company and with third parties. What are the pros and cons for consumers?

Pros -

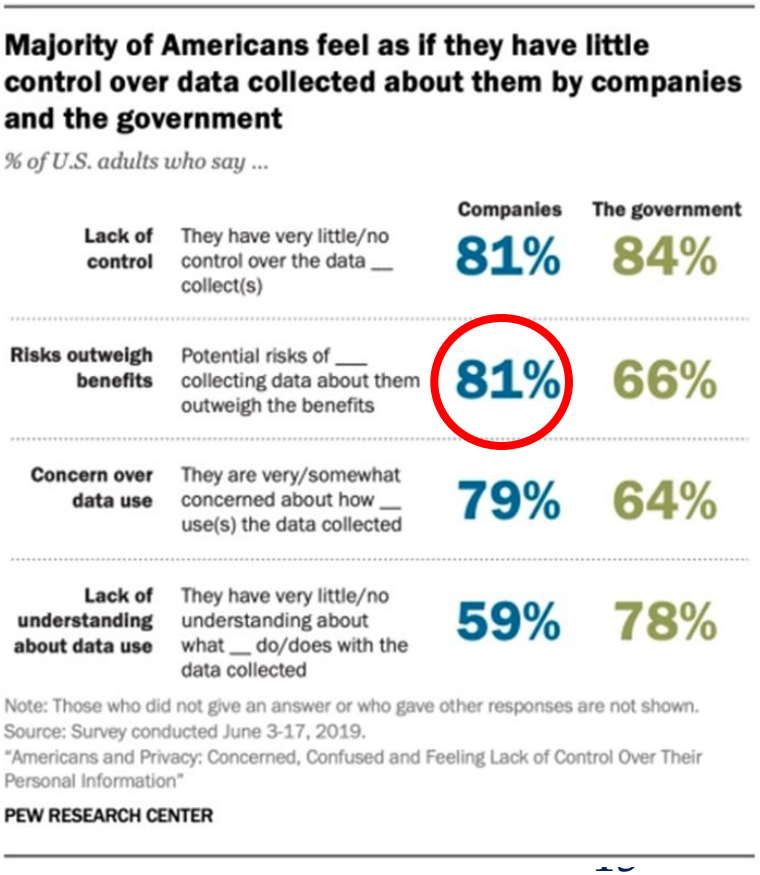
- Consumers may benefit from faster and cheaper payment systems.
- Availability of additional user data may open up the market to consumers without access to traditional financial services.
- Financial risks for both users and platforms may be reduced due to more data and analysis.

Cons –

- Companies may engage in invasive financial surveillance of users.
- Companies may operate in a manner that interferes with fair, transparent, and competitive markets.
- Companies may not adhere to required consumer protections and fair lending practices.
- Users may not have control of what data is collected, how it is shared, or the ability to fix incorrect information.
- Access to new products for customers does not guarantee that the products will be better than existing products or non predatory products.

Most Americans do not understand the details of data harvesting and monetization, but they do feel the lack of control over their own personal data

- In fact, 81% of consumers conclude that **the risks of corporate data collection outweigh the benefits**.
- And 75% say there **should be more government regulation** of what companies can do with personal data.



https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

A framework for assessing data harvesting and use

- As explained by the US Department of Justice, the **Privacy Act of 1974**, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. Though this law focuses on federal agencies, it has become the basis of modern privacy legislation at the state level as well as internationally.

- At the core of the Privacy Act are the **Fair Information Practice Principles (FIPPs)**
  1. Collection Limitation
  2. Data Quality
  3. Purpose Specification
  4. Use Limitation
  5. Security Safeguards
  6. Openness
  7. Individual Participation
  8. Accountability

https://www.justice.gov/opcl/privacy-act-1974

https://iapp.org/resources/article/fair-information-practices/

3 FIPPs directly address the CFPB orders

- Collection Limitation Principle - There should be **limits to the collection of personal data** and any such data should be obtained by fair means and **with the knowledge or consent of the data subject.**

- Purpose Specification Principle -The **purposes for which personal data are collected should be specified before data collection and the subsequent use limited to the fulfillment of those purposes.**

- Use Limitation Principle - **Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject**

The FIPPs serve as the basis for privacy laws in the private sector such as the California Consumer Protection Act and the EU General Data Protection Regulation.

https://iapp.org/resources/article/fair-information-practices/

https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Put those 3 FIPPs into consumer-friendly language

- The Collection Limitation Principle – I want the company to **collect only what is necessary** and **clearly ask my permission to gather it.**
- The Purpose Specification Principle – I want the company to tell me **what my data will be used for** and **only use it for that purpose**.
- The Use Limitation Principle – And I **do not want the company to sell or use my data in any other way without my permission.**

The shorthand version of these FIPPs may be termed "data minimization" – personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

https://gdpr-info.eu/art-5-gdpr/

FTC Commissioner Slaughter on data minimization

- "Rather than focusing on opt-in versus opt-out, and whether privacy policies are clear enough, I believe we should be discussing the concept of **data minimization-**
  - a principle that would ensure companies can **collect only the information necessary to provide consumers with the service on offer**,
  - and **use the data they collect only to provide that service."**

https://www.ftc.gov/system/files/documents/public_statements/1592854/slaughter_statement_privacycon_7-27-21.pdf

How well do payment platforms follow the FIPPs?

We recommend that the CFPB examine the data provided by the payment platforms and ask whether companies follow these principles when harvesting and monetizing data. **Do companies-**

- **Collection Limitation Principle –**
  - **Ask** user permission to gather their personal data
  - **Limit** collection to the data needed for a transaction
- **Purpose Specification Principle -**
  - **Specify** the purposes for which their data will be collected
  - **Use** data only for the fulfillment of those purposes
- **Use Limitation Principle –**
  - **Ask** permission to use data for purposes other than those specified
  - **Ask** permission to sell, disclose, or share user data

We also recommend that the CFPB survey users about their concerns surrounding data harvesting and monetization

Some questions consumers may have about how companies use their data:

- I understand collecting direct data to complete a particular transaction, but why do you need indirect data? Where does indirect data come from?
- The company's privacy policy is long and complicated. Can you just tell me exactly what you do with my data? Why make the policy so complex?
- Companies talk about about artificial intelligence and data science. Can you explain how that analysis impacts me? How can it hurt me?
- Why do you sell or share my data with other companies that I have never heard of? What do they do with it? Can I trust them to keep my data safe?
- How much money do you make off my data? What benefit do I get out of you using my data for free? Shouldn't you pay me for my data?

Conclusion

- Thank you for the opportunity to give you our thoughts on this important topic. We look forward to your reporting.

- Steve Perkins PhD
  - PerkinsTexas@MSN.com
  - Former VP Client Services for Burke, Inc Marketing Research
  - Former Associate Dean of Graduate Programs in the School of Management at the University of Texas at Dallas
  - Certified Information Privacy Professional
- Ann Baddour
  - ABaddour@TexasAppleseed.org
  - Director of the Fair Financial Services Project at Texas Appleseed