



October 21, 2022

RE: FTC Seek Comments on Trade Regulation Rule on Commercial Surveillance and Data Security, R111004, Docket ([FTC-2022-0053](#))

Thank you for the opportunity to provide comments for the Federal Trade Commission's Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security. Advances in digital technologies have allowed the incessant monitoring of consumer behavior. We are concerned by the volume and variety of personal data that companies gather, use, and sell, mostly without consumer permission or knowledge. Although this extensive corporate surveillance impacts most aspects of our lives from the ads we see to healthcare, we are particularly alarmed by the potential abuses in financial decision making and by physical and financial safety harms for vulnerable populations. As more financial decisions are made by algorithms and artificial intelligence, companies may discriminate against protected categories, whether intentionally or not. Besides race, gender, and age, other categories such as survivors of domestic abuse and the elderly may also face harms due to a combination of uncontrolled data availability and unregulated statistical modeling.

In this comment we focus our recommendations for FTC action on three questions in the Advance Notice of Proposed Rulemaking:¹

- Which areas or kinds of harm, if any, has the Commission failed to address through its enforcement actions? (question 8)
 - **Ensure that online data uses, including artificial intelligence-based lending models, do not create disparate impacts on protected classes.**
 - **Protect survivors of domestic violence, the elderly, and traditional protected classes from financial harm, fraud, and abuse by expanding consumers' ability to control their data held and sold by data brokers.**
- To what extent should new trade regulation rules impose limitations on companies' collection, use and retention of consumer data? (question 43)
 - **Base new FTC commercial regulations related to gathering, using, and storing personal data on the Fair Information Practice Principles.**
- How should the Commission evaluate or measure algorithmic discrimination? (question 66)

¹ Trade Regulation Rule on Commercial Surveillance and Data Security
<https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security>

- **Research how combining extensive consumer data with advanced statistical models increases or decreases discrimination in financial decision making.**

Current practices enable abuse of protected and vulnerable individuals

At its core, privacy is “controlling how personal information is used and ensuring that this information is not used against the interests of individuals.”

—Cameron F. Kerry, Brookings²

To begin to understand the vast amount of data companies collect on us, we must consider a major group of players in this space, data brokers. Data brokers collect personal data on individuals and then sell that data to third parties and anyone willing to pay, even though the data broker has no relationship with the person surveilled. This transaction happens without the individual’s knowledge or participation. To date, there are approximately 4000 data brokers active in the world, generating over \$200 billion in revenue annually.³ For example, consider Acxiom, a large data broker that holds 11,000 pieces of data on 2.5 billion people in 62 countries.⁴ That data includes demographics, religion, political party, credit card purchases, income, net worth, health concerns, media usage, and much more. With this detailed, sensitive data, Acxiom can assign individuals to a marketing segment, or audience, such as “Big Spender Parents” who are middle-aged, traditional family households with children, with an average income of \$207,000. These results could then be sold to marketers who produce advertisements targeted to that segment, lenders making credit decisions, companies assessing job seekers, or apartment managers reviewing housing applications – all without the individual’s knowledge or permission. In 2014, the FTC called for more transparency and accountability for data brokers, but nothing has changed at the federal level.⁵

Consumers are increasingly aware of the harmful ways that personal data can be used. They know that companies have the upper hand in dictating how their data is collected, analyzed, and shared. A Pew Research Center study in 2019 found that 79% of Americans expressed concern about how companies use their data.⁶ Even the Internet Association, a lobbying group representing Google, Amazon, and Facebook, among others, acknowledged in 2020 that 85% of consumers say they should have more control over the personal information they share online.⁷ Existing regulations do not protect the collection and use of consumer’s personal data because at

² Kerry, Cameron *et. al.*, published by the Brookings Institution (June 2020) [Bridging the Gaps: A path forward to federal privacy legislation](#).

³ What Are Data Brokers – And What Is Your Data Worth? <https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/>

⁴ See: <https://www.acxiom.com/>

⁵ Federal Trade Commission, “Data Brokers: A Call for Transparency and Accountability” (May 2014), <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>

⁶ Brook Auxier, Lee Raine, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.” Pew Research Center, (November 15, 2019).

⁷ The Internet Association, “Survey on Data Privacy” 2020 https://internetassociation.org/wp-content/uploads/2020/05/IA_Survey-On-Data-Privacy.pdf

the federal level, the United States does not have a comprehensive privacy law that governs the collection, use, and sale of consumer information. Professors Daniel Solove and Paul Schwartz, George Washington University Law School and University of California, Berkeley, respectively, describe U.S. privacy statutes as a “fragmented, inconsistent patchwork of laws.”⁸

There are federal laws that regulate the use of financial information, such as Gramm-Leach-Bliley Act (enforced by the FTC) and the Fair Credit Reporting Act (enforced by the Consumer Finance Protection Bureau),⁹ but the Government Accountability Office (GAO) has recommended changes to consumer privacy laws to keep pace with market developments and to implement broad internet privacy legislation. To date, Congress has done neither. As the GAO reported, “although the FTC generally has addressed internet privacy through its unfair and deceptive practices authority, and other agencies have used industry-specific statutes, there is no comprehensive federal privacy statute with specific internet privacy standards for the private sector....new and more advanced technologies and changes in the marketplace for consumer information have vastly increased the amount and nature of personal information collected and the number of parties using or sharing it.”¹⁰

There are several laws that prohibit discrimination based on race and other personal characteristics, including the Civil Rights Act, Fair Housing Act, and Voting Rights Act, however, agencies protecting data privacy often do not consider protecting civil rights, and agencies protecting civil rights do not consider protecting data privacy. Because of this disconnect, consumer privacy advocates recommend focusing on the intersection of privacy and civil rights.¹¹ In an example of how technology platforms can illegally use data to discriminate against individuals, a ProPublica investigation in 2016 found that Facebook allowed marketers to exclude African Americans from viewing some of their advertisements for houses. Later, the Department of Justice took up the case and accused Facebook of violating the Fair Housing Act. In the settlement, Facebook, now Meta, “agreed to eliminate features in its advertising business that allow landlords, employers and credit agencies to discriminate against groups of people protected by federal civil rights laws.”¹² This case would not have been brought about without ProPublica viewing consumer protection from the intersectional perspective of privacy rights and civil rights. Given the traditional legal separation between privacy rights and civil rights,

- **We recommend that the FTC ensure that online data uses, including artificial intelligence-based lending models, do not create disparate impacts on protected classes.**

⁸ ALI Data Privacy: Overview and Black Letter Text (January 24, 2020). UCLA Law Review, Vol. 68, 2020, <https://ssrn.com/abstract=3457563> or <http://dx.doi.org/10.2139/ssrn.3457563>.

⁹ JDSupra, “What Fintech Companies Need to Know About Key Federal Privacy Requirements” 2022 <https://www.jdsupra.com/legalnews/what-fintech-companies-need-to-know-2217024/>

¹⁰ “Consumer Privacy: Changes to Legal Framework Needed to Address Gaps.”

GAO-19-621T. Published by the U.S. Government Accountability Office (June 11, 2019).

¹¹ See, for example: Steve Perkins and Ann Baddour, *Texas at a Crossroads: Protecting Privacy and Civil Rights* (April, 2022).

¹² ProPublica, “Facebook Finally Agrees to Eliminate Tool That Enabled Discriminatory Advertising” 2022 <https://www.propublica.org/article/facebook-doj-advertising-discrimination-settlement>

Equally important is the FTC's duty to consider the harmful human impacts that a lack of data privacy protections causes, especially for vulnerable populations, such as survivors of domestic violence. In Texas, one in three individuals will experience domestic violence in their lifetime.¹³ While domestic violence is often understood as physical and emotional violence, economic abuse – federally defined in the Violence Against Women's Reauthorization Act as "behavior that is coercive, deceptive, or unreasonably controls or restrains a person's ability to acquire, use, or maintain economic resources to which they are entitled, including using coercion, fraud, or manipulation," is a dominant component that further restricts a survivor from successfully leaving an abusive relationship.¹⁴ In the first half of 2020, nearly one in three Texans who called the National Domestic Violence Hotline reported economic or financial abuse.¹⁵ The rapid growth of technology brings both benefits and risks to the well-being and security of survivors. Privacy is crucial for a survivor's safety, and privacy concerns for a survivor's physical safety and self-sufficiency manifest in an array of ways, ranging from fear of seeking shelter due to a lack of trust in confidential data collection and information processes to experiencing homelessness to stay off the technological radar. Under the scattered federal approaches to data privacy and in combination with expansive data collection, sharing, and selling, survivors are finding it increasingly difficult to maintain any form of privacy.

With this new digital age of innovative technology comes ingenious ways for abusers to gain access to their victim's personal identifying information and, as a result, have ongoing impacts on a survivor's financial stability and physical safety. Economic exploitation is one way that domestic violence abusers can use the vast collection of data available to continue to harass and harm survivors both when they are in an abusive relationship and long after they have left the relationship. Data brokers have enabled abusive partners to access a survivor's personal identifying information and incur debts in the survivor's name. This can have significant impacts on a survivor's physical and financial stability. In a 2021 nationwide study by the Center for Survivor Agency and Justice (CSAJ) on domestic violence and economic well-being, participants were asked about their experiences with economic restriction (e.g., the abuser kept the survivor from going to work) and exploitation (e.g., the abuser took out a credit card in the survivor's name) perpetrated by their abuser. Among the survivors surveyed, 97% experienced economic abuse.¹⁶

A specific form of financial abuse called *coerced debt* can burden the survivor with bad credit caused by the abuser. Coerced debt, defined as non-consensual, credit-related transactions occurring in an abusive intimate relationship - is a form of identity theft where an abuser obtains credit using the survivor's identifying information through threats, fraud, and/or coercion.¹⁷

¹³ Crime in Texas," Family Violence, Texas Department of Public Safety (TDPS), 2017.

¹⁴ See 34 USC 12291: Definitions and grant provisions, <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title34-section12291&num=0&edition=prelim>

¹⁵ National Domestic Violence Hotline, Texas State Report, January-June 2020, available at <https://www.thehotline.org/stakeholders/impact-and-state-reports/>.

¹⁶ Adrienne Adams and Sara Wee, "Domestic Violence and Economic Well-being Study." Center for Survivor Agency and Justice, (April 2021).

¹⁷ Angela K. Witten, "Coerced Debt: The Role of Consumer Credit in Domestic Violence." California Law Review, Volume 100, pp. 1-74, (June 1, 2012).

Although coerced debt is often associated with survivors of domestic violence, it is also found in cases of elder financial abuse,¹⁸ financial abuse of a person with disabilities, or child abuse/exploitation of youth. Even after a survivor has left their abuser, the abuser can financially exploit their victim by taking out coerced debts – even if they no longer have physical access to their victim’s important information – by purchasing their data through data brokers. When an abusive partner takes out a coerced debt in a survivor’s name, oftentimes the survivor is not aware that the debt has been taken out. Even if the survivor knows about the debt, they often are unable to address the debt due to their abuser maintaining strict control over their finances. Consequently, coerced debts can lead to negative consumer credit reports. Because of the growing role that credit reports play in financial wellbeing – from attaining employment to renting an apartment – coerced debt can have devastating impacts on a survivor's long-term financial wellbeing and security. Additionally, the CSAJ study found that over one-third of survivors reported an abuser taking out a loan or buying something on credit in the survivor’s name without permission. This type of abuse is easier to perpetrate and can be more damaging and long-lasting because of the lack of data privacy protections and, in turn, the ease of accessing and using another person’s data.

In addition to the economic exploitation that can occur without crucial data privacy protections, abusers take advantage of the sale of location, address, and other personal identifying data available online to stalk, harass, and locate a survivor, which can have detrimental outcomes to a survivor’s safety. The most infamous example of this is when Amy Boyer’s stalker, Liam Youens, purchased Amy’s birthdate, social security number, and home and workplace address from data broker Docusearch in 1999. Youens then used this information to locate Amy at her place of work, where he fatally shot her.¹⁹ Amy’s tragic death is not a one-off occurrence of the lengths that abusive individuals will go to locate and further perpetrate abuse against their victims. More than twenty years later, survivors still face similar threats from abusers, as it has become cheaper and easier to access personal information in a legal environment without consistent data control or protections. Because of the vulnerable status of survivors of domestic violence, the elderly, and other populations, and the imperative need to protect their data from an abuser,

- **We recommend that the FTC protects survivors of domestic violence, the elderly, and traditional protected classes from financial harm, fraud, and abuse by expanding consumers’ ability to control their data held and sold by data brokers.**

¹⁸ S.795 - 111th Congress (2009-2010): Elder Justice Act of 2009, S.795, 111th Cong. (2009)

¹⁹ EPIC, “The Amy Boyer Case.” (June 15, 2006).

Commercial surveillance of consumers

“All data is credit data. We just don’t know how to use it yet.”

—Doug Merrill, ZestFinance 2012²⁰

Even beyond the enormous amount of data collected by brokers like Acxiom, lenders may also take into consideration “non-financial” data when making credit decisions. For years, many lenders based their decisions on traditional financial data, specifically a borrower’s FICO score. Lenders might use a simple decision-making rule: applicants with a score above a certain level would receive a loan, and those below that level would not.²¹ However, the CFPB estimates that almost 20% of American adults do not have a FICO score, primarily due to insufficient financial history. This group of individuals is essentially “invisible” to the credit system, making it very difficult for them to obtain credit, which is a dominant factor in building and maintaining financial stability.²²

Because of this invisibility, some lenders now assess “alternative data” in their credit making decisions, which can include everything from utility payments and cash flow analysis to social media activity and internet browser history.²³ The hope has been that alternative data might offer a way for “invisibles” to be scored based on non-traditional data and considered for credit opportunities, thus broadening financial inclusion. The downside of using alternative data, however, is the possibility that this type of data can hurt borrowers’ chances of fairly being scored or receiving credit products.²⁴ Given the availability of more data and stronger decision-making models, traditional consumer credit reports could become obsolete, possibly allowing companies to avoid Fair Credit Reporting Act regulations that are meant to protect consumers from abusive and predatory credit practices.²⁵

There is a framework for remedying this uncontrolled data gathering and unregulated data use. In 1974, Congress passed the Privacy Act which governs the collection, storage, use, and dissemination of personal information by federal agencies.²⁶ The Privacy Act established eight Fair Information Practice Principles (FIPPs) – the appendix outlines the principles. Of those

²⁰ “Just the Facts. Yes, All of Them” The New York Times 2012

<https://archive.nytimes.com/query.nytimes.com/gst/fullpage-9A0CE7DD153CF936A15750C0A9649D8B63.html>

²¹ Matthew Bruckner “The Promise and Perils of Algorithmic Lenders’ Use of Big Data” 2018

<https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=4192&context=cklawreview>

²² Data Point: Data Invisibles

https://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf

²³ Robinson + Yu, “Knowing the Score: New Data, Underwriting, and Marketing in the Consumer Credit Marketplace” 2014

https://www.upturn.org/static/files/Knowing_the_Score_Oct_2014_v1_1.pdf

²⁴ Nikita Aggarwal, “The Norms of Algorithmic Credit Scoring, 2021

<https://www.cambridge.org/core/journals/cambridge-law-journal/article/abs/norms-of-algorithmic-credit-scoring/23C9802EEA5EC6F6872512CB7AABC793>

²⁵ Nikita Aggarwal, Big Data and the Obsolescence of Consumer Credit Reports, 2019

<https://blogs.law.ox.ac.uk/business-law-blog/blog/2019/07/big-data-and-obsolescence-consumer-credit-reports>

²⁶ US Department of Justice, Privacy Act of 1974, USC 552a

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

eight principles, consider how three of them could apply to companies making financial decisions about individuals:

- Collection limitation – do not gather more data than is needed,
- Purpose limitation – do not use that data for another purpose, and
- Use limitation – do not disclose that data to other companies.

Consumers understand that they must provide some data to companies they do business with, but based on the FIPPs, the company should not collect more data than is necessary to complete the specific service the borrower seeks. The company should explain exactly what they will do with the data and use it only for that purpose. The company should not sell, transfer, or share personal data with other parties, including data brokers and online platforms, without explicit consent from the consumer.

The FIPPs served as the basis for FTC privacy recommendations in 2000²⁷ and White House privacy recommendations in 2012.²⁸ They have also been applied to commercial use of personal data under the California Consumer Privacy Act and the European Union’s General Data Protection Regulation.²⁹ Because of the current lack of comprehensive data privacy protection standards,

- **We recommend that the FTC base new commercial regulations related to gathering, using, and storing personal data on the Fair Information Practice Principles.**

To this effect, FTC rules could go a long way toward protecting personal data through better regulation of data collection, sharing, and selling practices.

Algorithmic decision making

“Opaque and invisible models are the rule, and clear ones very much the exception...”

—Cathy O’Neil, author, *Weapons of Math Destruction*³⁰

Armed with an ocean of data, companies now employ advanced statistical models to make decisions. Financial services companies have developed sophisticated algorithms to make credit decisions. Algorithmic credit scoring often employs machine learning techniques that analyze large volumes of data to find correlations that could help predict a borrower’s creditworthiness. However, the opacity and complexity of these methods can make it difficult to determine

²⁷ Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress, 2000

<http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>

²⁸ The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Washington, D.C.: Feb. 23, 2012)

<https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf>

²⁹ 50 years and still kicking: An examination of FIPPs in modern regulation, 2019

<https://iapp.org/news/a/50-years-and-still-kicking-an-examination-of-fipps-in-modern-regulation/>

³⁰ Cathy O’Neil, *Weapons of Math Destruction*, (2016).

<https://www.penguinrandomhouse.com/books/241363/weapons-of-math-destruction-by-cathy-oneil/>

whether the system has relied on protected borrower characteristics (or proxies for them) to reach a credit decision. In addition, given the availability of data and the precision in modeling, the lender can more easily target borrowers with unfavorable credit offers at their moments of extreme vulnerability, such as an emergency or illness.³¹

The CFPB laid out potential risks associated with the combination of alternative data and advanced modeling in credit decision making: “Machine learning algorithms that sift through vast amounts of data could unearth variables, or clusters of variables, that predict the consumer’s likelihood of default (or other relevant outcome) but are also highly correlated with race, ethnicity, sex, or some other basis protected by law... The use of alternative data and modeling techniques could potentially lead to disparate impact on the part of a well-intentioned lender as well as allow ill-meaning lenders to intentionally discriminate and hide it behind a curtain of programming code.”³²

The combination of enormous amounts of data and cutting-edge modeling could lead to greater financial inclusion, but the potential for discrimination and inefficiency exist. To date, there has been little published, empirical research on the consumer harms and benefits of using these systems. One study of financial technology, or “fintech,” lending concluded that while algorithmic lending reduced discrimination compared to face-to-face lenders, it did not eliminate discrimination in the pricing of loans. The study found that Hispanic and African American borrowers pay 5.3 basis points more in interest for purchase mortgages and 2.0 basis points for refinance mortgages originated on Fintech platforms.³³

Recently, the Biden administration published a “Blueprint for an AI Bill of Rights,” which documents how artificial intelligence has contributed to discrimination in determining college loans, hiring, selecting college majors, predicting prison recidivism, monitoring social media, calibrating search engines, presenting targeted advertising, setting up TSA body scanners, proctoring test taking by disabled students, making healthcare decisions, and much more. The use of algorithms in financial systems include loan applications, credit scoring, and insurance risk assessment, among others. The Blueprint suggests testing a system before it is launched and conducting on-going evaluation in the field to protect against algorithmic discrimination.³⁴

The Administration’s report, among other similar findings, can be used by financial firms as justification that the benefits of using AI in lending practices outweigh the costs, emphasizing the positives of data driven, algorithmic decision systems. However, the issue lies in that there is

³¹ Nikita Aggarwal, Algorithmic Credit Scoring and the Regulation of Consumer Credit Markets, 2018 <https://blogs.law.ox.ac.uk/business-law-blog/blog/2018/11/law-and-autonomous-systems-series-algorithmic-credit-scoring-and>

³² CFPB, Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process, 2017 https://files.consumerfinance.gov/f/documents/20170214_cfpb_Alt-Data-RFI.pdf

³³ Robert Bartlett, Adair Morse, Richard Stanton, and Nancy Wallace, “Consumer-Lending Discrimination in the FinTech Era” 2019 <https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf>

³⁴ Blueprint for an AI Bill of Rights <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>

little empirical, objective evidence to support or refute the efficacy of these systems. Given the paucity of third-party research,

- **We recommend that the FTC research how the combination of extensive consumer data with advanced statistical modeling increases or decreases discrimination in financial decision making.**

There is a clear need for research centered on whether financial firms reduce or exacerbate discrimination when using state-of-the-art data and models. In 2021, the San Francisco Federal Reserve outlined several research questions around studying “the promise and pitfalls of financial technology for fostering racial equity and greater financial inclusion.”³⁵ Some empirical research has been conducted - the FinRegLab concluded that companies may have to tradeoff between fairness practices and predictive performance, since models including protected characteristics may lead to greater predictive accuracy.³⁶ In all circumstances, consumers should know both the costs and benefits of financial technology when making financial decisions.

Conclusion

“Inputs go into the black box and outputs come out, but we do not know how they transform the inputs into the outputs... and once we get a sense of how they are transformed, we have very little chance of influencing it for the better.”

—Frank Pasquale, “Big data, algorithms and discrimination in the black box society,” 2018³⁷

Americans face relentless corporate surveillance, armed only with feeble data protections. Companies collect, use, and transfer immense troves of personal data with minimal consumer consent or knowledge, and at the same time, consumers endure some of the weakest data privacy laws in the developed world. It did not have to turn out this way. We believe our recommendations will empower Americans to enjoy the benefits of technology and avoid its worst discrimination.

³⁵ Fintech, Racial Equity, and an Inclusive Financial System - Volume 15, Issue 2, San Francisco Fed, 2021 <https://www.frbsf.org/community-development/publications/community-development-investment-review/2021/august/fintech-racial-equity-inclusive-financial-system/>

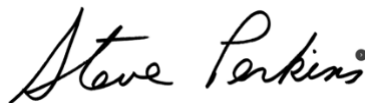
³⁶ FinRegLab, “Machine Learning Explainability & Fairness: Insights from Consumer Lending” 2022 https://finreglab.org/wp-content/uploads/2022/04/FinRegLab_Stanford_ML-Explainability-and-Fairness_Insights-from-Consumer-Lending-April-2022.pdf

³⁷ Frank Pasquale, “Big data, algorithms and discrimination in the black box society” 2018 <https://anchor.fm/digital-sociology-podcast/episodes/Episode-18-Frank-Pasquale--big-data--algorithms-and-discrimination-in-the-black-box-society-e2q408>

In summary, our recommendations to the FTC are:

1. Ensure that online data uses, including artificial intelligence-based lending models, do not create disparate impacts on protected classes.
2. Protect survivors of domestic violence, the elderly, and traditional protected classes from financial harm, fraud, and abuse by expanding consumers' ability to control their data held and sold by data brokers.
3. Use the Fair Information Practice Principles as the basis for commercial surveillance regulations on gathering, using, and transferring personal data.
4. Institute a research-centered agenda to examine how the combination of consumer data and advanced statistical models impact discrimination in financial decision making.

We appreciate the FTC's interest in prioritizing consumer protection through inquiring about better means to protect consumers in the face of commercial surveillance and algorithmic decision making.



Steve Perkins PhD, Appleseed pro bono partner, former Associate Dean of Graduate Programs in the School of Management at The University of Texas at Dallas



Briana Gordley, LMSW
Policy Analyst, Texas Appleseed

APPENDIX

Appendix A – Fair Information Practice Principles (FIPPs) Table

Fair Information Practice Principles (FIPPs)	
Principle	Description
Collection limitation	The collection of personal information should be limited, obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose limitation	The purposes for the collection of personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for purposes other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles