Credit Bureaus in the Digital Age:

Recommendations for Policy Makers

By Ann B. Schnare

AB Schnare Associates LLC
3010 P Street NW
Washington DC 20007

Ann Schnare holds a Ph.D. in economics from Harvard University and is President of AB Schnare Associates, LLC. She served as Senior Vice President for Corporate Relations and Vice President for Housing and Financial Research at Freddie Mac from 1993 to 2000, and was a member of the company's Operating Committee. Since leaving Freddie Mac, Dr. Schnare has provided a range of consulting services, focusing on housing finance reform, financial regulation, mortgage servicing, credit scoring, and alternative measures of credit risk. Funding for this paper was provided by Equifax. However, the views expressed herein are those of the author and do not necessarily reflect the opinions of Equifax.

Executive Summary

This paper examines the role of credit bureaus in the digital age, and how this role is being affected by the explosion of personal data and its rapidly growing use for a wide variety of decisioning and marketing purposes. Its major objectives are to provide policy makers with a better understanding of the importance of credit bureaus to consumers and the broader economy, how the data that credit bureaus provide sets them apart from other large-scale data aggregators, and the implications of these differences for the formulation of public policy with respect to credit bureaus, as well as to broader issues related to consumer privacy and data security.

The paper begins with a general discussion of key policy issues related to the use and protection of personal data, including the trade-offs that inevitably arise when balancing concerns over consumer privacy and data security with the desire for innovation. It then focuses on the important role that credit bureaus play in the functioning of modern economies, the legal and regulatory regime that currently governs the use and distribution of consumer reports, and a number of important trends that could affect the future of credit bureaus, including the use of alternative data to augment or replace traditional credit reports, the development of increasingly sophisticated analytic tools, and the rise of Fintechs and mobile banking web applications (apps). The paper ends with some broad conclusions and policy recommendations, which are summarized below:

➢ First, while it is difficult, if not impossible, to predict the structure of the credit reporting industry going forward—let alone the types of data that will ultimately be used in credit decisions—as long as there is a demand for credit, there will likely be a need for the services that credit bureaus provide, namely, an objective and comprehensive view of the consumer's credit history. As such, concepts such as "opting in" or "opting out" simply do not apply to credit reports. Policy makers need to recognize this important distinction as they attempt to address broader issues of consumer privacy, and maintain explicit "carve outs" for credit reporting purposes.

➢ Second, the U.S. legal and regulatory regime that currently governs the use and distribution of credit reports is extremely robust, and has successfully withstood the test of time despite dramatic advances in computer technology and the ability to store and analyze data. By focusing on the acceptable uses of the data—and by ensuring transparency by giving consumers access to their credit reports—this basic approach can and should provide the legal and regulatory guardrails for credit reporting going forward, regardless of how the industry eventually evolves or the data that are used to measure "creditworthiness." Further efforts to improve the existing system should focus on consumer education and the ability to redress errors, as well as on the kinds of "non-traditional" data that can be—and cannot be—used in FCRA- and ECOA-covered transactions.

➤ Third, some 45 million consumers today either do not have a credit file or have files that are "too old" or "too thin" to receive a traditional credit score. To better serve these so-called "credit invisibles," policy makers should continue to explore ways to encourage the reporting of telecom, utility and rental data, recognizing that such reporting must capture both positive and negative payment histories in order to maximize the benefits to consumers. While some consumers might see a reduction in their credit scores, research has consistently shown that the inclusion of such data will lead to a net increase in consumers' access to credit, particularly for minorities and lower-income consumers.

➤ Fourth, a growing number of Fintechs are beginning to use non-financial personal data as inputs to FCRA-covered transactions. To encourage innovation and avoid "regulation by enforcement," policy makers should take steps to develop regulatory guidance on the use of various types of personal data for decisioning purposes. They should also support the Treasury's call for the creation of so-called "sandboxes" where specific applications can be tested and evaluated without fear of repercussion. Policy decisions regarding the use of particular kinds of personal data for credit decisions should be based on more than the data's predictive power. They should also reflect broad social and ethical values about the society in which we want to live.

➤ Fifth, the focus of the Fair Credit Reporting Act (FCRA) on regulating the use of personal data, as opposed to its collection, can provide a model for more general privacy regimes. It is tempting to assert that consumers should have the ultimate say over the collection and use of their data. However, the potential personal, economic and social benefits that can arise from the innovative use of data may at times conflict with, and often outweigh, the benefits of consumer control. In the end, it is virtually impossible for anyone to know what kinds of data or applications will prove to be valuable going forward. For these and other reasons, policies designed to address broader issues of consumer privacy should focus on the use, rather than the collection of personal data. Uses that are judged to be inconsistent with existing laws or with broader social and ethical norms should be explicitly prohibited and incorporated into applicable laws.

➤ Sixth, the growing incidence of cyber-attacks underscores the need for national data security standards governing the protection of personal data, as well as responses to data breaches. There could conceivably be technical solutions in the future that would render personal data impervious to potential hackers or make the information worthless in the event of a data breach. However, because even the best technologies will inevitably become obsolete, Congress should take steps to develop national data security standards that focus on the principles and processes that need to be put in place to protect a consumer's data, not on the specific technologies that should be employed.

➤ Finally, absent Congressional action, there needs to be greater clarity and certainty regarding the specific data security standards that are applicable to credit bureaus, and greater coordination among the relevant regulatory agencies at both the state and federal

levels. While credit bureaus are subject to the FTC Safeguards rule, these standards are very broad, and no federal agency currently has the authority to routinely supervise credit bureaus for compliance with these standards. At a minimum, policy makers should adopt Treasury's recent recommendation calling for the relevant regulatory agencies to coordinate their actions with respect to the security of credit bureau data, and for Congress to assess whether further authorities are needed—including the authority to conduct routine compliance reviews. Otherwise, the patchwork of overlapping data security laws, regulations and enforcement actions is likely to continue—an outcome that is not in the long term interests of consumers, creditors or the broader economy.

The remainder of this paper describes the issues in more detail, as well as the reasoning that underlies these basic conclusions and policy recommendations.

1.0 Background

The onset of the digital economy, the monetization of "big data," and increasingly sophisticated analytic tools have led to numerous public policy concerns related to the vast amounts of consumer data now routinely collected by entities ranging from small "mom and pop" shops to large financial institutions to internet giants such as Google, Facebook and Amazon. Every time a consumer uses their cell phone, shops online, posts on social media, conducts a web search, accesses the "internet of things" or purchases an item from a bricks-and-mortar store, they are likely to leave a digital footprint that can be used or sold for a variety of purposes, both good and bad.

Not surprisingly, rarely a week goes by without some mention of a data breach or an inappropriate use of consumer data. Cybersecurity has become a major concern that is affecting virtually every sector of the economy. Facebook's recent data breach, the hacking of Office of Personnel Management and Internal Revenue Service data bases, along with numerous other examples from both the government and private sectors illustrate the vulnerabilities of personal data to both external and internal threats. According to one estimate, there were more than 275 million breaches of personally identifiable information (PII) in 2017 alone, almost as high as the total number of PII breaches that occurred in the previous six years (at least 320 million). In 2018, the pace of breaches continued to accelerate, resulting in 345 million consumer PII records being compromised through October.[1] Given that there are roughly 248 million adults in the country today, the average consumer has likely had their information hacked.

While the U.S. Department of Treasury ("Treasury") recently issued a report that called for Congress to enact national data security standards,[2] similar efforts in the past have failed to gain much traction on the Hill. A 2019 report by the Congressional Research Service (CRS) provides an overview of the current federal approach to cybersecurity, which is based on a complex patchwork of laws that are largely targeted to specific government agencies and the private entities they oversee.[3] According to the CRS, while there are numerous statutes that address various aspects of cybersecurity, "these statutes primarily regulate certain industries and subcategories of data. The FTC fills in some of the statutory gaps by enforcing a broad prohibition against unfair and deceptive data protection practices. But no single federal law comprehensively regulates the collection and use of consumers' personal data".[4]

---

[1] Personally identifiable information (PII), as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. These statistics do not include other consumer data that was stolen through breaches affecting account IDs, credit card numbers, email addresses, passwords and security questions for authentication. See https://www.identityforce.com/blog

[2] U.S. Treasury, *A Financial System that Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation.* July 2018. https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf

[3] Congressional Research Service, "Data Protection Law: An Overview" March 25, 2019. https://crsreports.congress.gov/product/pdf/R/R45631.

[4] Ibid. Summary.

There are also fundamental questions about how a consumer's data should be used, and the control that the consumer should have over someone's ability to use their personal data. Cambridge Analytica's use of Facebook data to influence the 2016 Presidential election is perhaps the most vivid illustration of what can go wrong. However, there are numerous other "gray areas" where the potential benefits from the use of a consumer's personal data for certain purposes might well outweigh the potential costs. For example, should information on a consumer's spending patterns, cell phone use, Facebook friends or education be used as an input to credit decisions even if the inclusion of such data has statistically proven predictive power?

Such concerns have led countries around the globe to seek ways to protect the privacy of their citizens while facilitating the convenience and innovation that can occur from the creative use of big data and increasingly powerful analytic tools. A number of regulatory regimes have emerged that attempt to give consumers more control over the use of their personal data. Perhaps the most extensive one to date is the General Data Privacy Regulation (GDPR), which became effective in May 2018 and applies to all companies doing business in the European Union. Although similar efforts have stalled in the United States at the federal level, Congressional inaction has caused a number of states to attempt to fill the void. The most recent example is California's Consumer Privacy Act of 2018, which is similar to the GDPR and scheduled to go into effect in 2020.

While policy approaches and concerns over the collection and use of big data are multifaceted in nature, they essentially boil down to three overarching questions:

- What rights should consumers have over the collection and use of their personal data ("*consumer privacy*" or *"consent")?*

- How should a consumer's data be protected once it is obtained ("*data security"*)?

- What are appropriate and inappropriate uses of a consumer's personal data ("*acceptable use"*)?

Answers to these questions will inevitably depend on the type of data being collected, as well as on the various costs and benefits that may arise from restricting their potential use. These tradeoffs will reflect more than economics. They will also reflect ethical and social judgments regarding the type of society we want to have. Similar to laws against racial redlining in the mortgage industry, the fact that something is statistically valid does not always mean it is desirable to base decisions on it.

From the consumer's perspective, issues related to consumer consent, data security and acceptable use are either unknown or typically viewed as one and the same. However, from a public policy perspective, the three are very different and may at times conflict. For example, with today's rapidly advancing technologies, the only sure way to protect a consumer's personal data from a potential breach is to make the data totally inaccessible to any potential user, be it the government, a research institute, or a private company. At best, such a policy

would stifle innovation and deny consumers the potential benefits that innovative use of their data might bring. At worst—as would be the case for consumer credit reports—it would bring a virtual halt to financial transactions, limiting both the flow of payments as well as consumers' access to credit. As illustrated in Figure 1, the stricter the regulatory regime, the smaller the set of data that can be put to work for potentially beneficial social and economic purposes.

Figure 1: Data Use Is Determined by the Intersection of Key Requirements
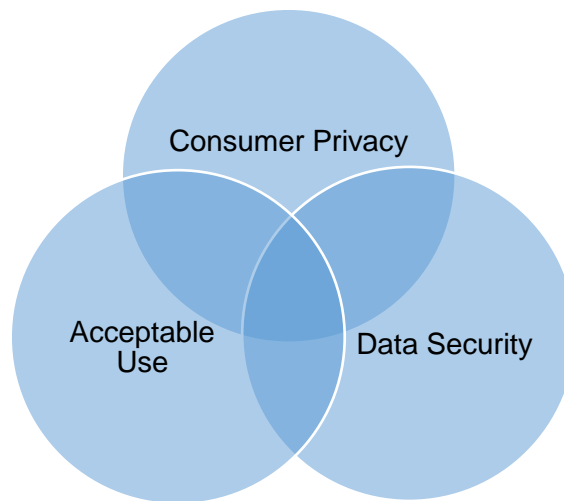
Questions regarding consumer consent, acceptable use and data security apply to virtually every type of consumer data. However, they are particularly germane to the kinds of personal financial data that are collected, maintained and distributed by consumer credit reporting agencies (CRAs), otherwise known as credit bureaus. Credit bureaus compile information on the credit histories of individual consumers and then sell the data to potential creditors and other qualified third parties.[5] The data contained in a consumer's credit report are supplied on a voluntary basis by banks and other creditors, or collected from public records. Credit reports typically provide detailed information on an individual's various credit lines (e.g., payment history, outstanding balances, credit limits, etc.), any reported collections, bankruptcies, or foreclosures, and a list of entities that have requested the reports for the evaluation of a new credit application (otherwise known as "hard credit inquiries").[6] In some cases, credit files also contain information on a consumer's payment history on other recurring bills (e.g., utility, telecom, rent), although the coverage is currently limited. While

---

[5] For a detailed discussion of how credit bureaus operate, see Consumer Financial Protection Bureau (CFPB), "Key Dimensions and Processes in the U.S. Credit Reporting System: A review of how the nation's largest credit bureaus manage consumer data," December 2012. https://www.consumerfinance.gov/data-research/research-reports/key-dimensions-and-processes-in-the-u-s-credit-reporting-system/

[6] "Soft inquiries" are visible only to the consumer, and indicate if the consumer's record has pulled a record for a non-credit granting reason, such as when a consumer reviews her own records, for credit counseling, or a creditor's review of existing account holders.

credit files have "headers" that are used to identify individual consumers (e.g., name, address, social security number, etc.), they do not contain demographic data such as race, ethnicity, national origin, religious affiliation, or marital status.

Almost fifty years ago—long before the public release of the internet and the subsequent birth of the digital age—the sensitive nature of credit reports and growing concerns over consumer privacy gave rise to the 1970 Fair Credit Reporting Act (FCRA). The FCRA—which was substantially amended in 1996, 2003 and again in 2018—was designed to address basic issues of consumer privacy (or consent) by establishing strict limitations on who can access the data and how it can be used. It also established a number of consumer rights that were designed to ensure the transparency and accuracy of the data contained in credit reports. While technology has changed dramatically since its original enactment, the FCRA—along with a series of anti-discrimination laws and other legislative and regulatory enhancements—continues to provide the basic framework for ensuring the "fairness, accuracy, and privacy" of the personal information contained in a consumer's credit file.

2.0 The Role and Importance of Credit Bureaus

Most consumers have relatively little understanding of what credit bureaus do or the role that they play in various aspects of their lives. When things go wrong, many consumers blame the credit bureaus for their inability to get a loan or for reporting negative information that they view as inaccurate or essentially beyond their control (e.g., medical collections, unemployment, or divorce).[7] Yet credit bureaus inarguably play a critical and positive role in the functioning of modern economies—so important that the International Finance Corporation, a member of the World Bank Group, launched an initiative in 2001 to foster the development of private credit bureaus in emerging markets around the world. By providing an objective and comprehensive view of a consumer's use of credit, credit bureaus reduce the risk that is inherent in lending decisions, thereby enabling creditors to serve a broader segment of the population at a lower cost.

2.1 The History of Consumer Credit Bureaus in the United States

Consumer credit reporting agencies emerged in the United States in the late-1800s in response to the onset of the industrial revolution and the vast population shifts that followed the end of the Civil War.[8] As merchant lenders found it increasingly difficult to rely on personal relationships or letters of reference as a basis for extending credit to local businesses and individuals, they began to form small cooperatives to share information on their different customers. In the beginning, credit reports were simply a list of individuals who had not paid their bills. Over time, however, credit reports became more detailed, and often contained personal information such as the consumer's marital status, religious affiliation, or membership in a local civics organization.

---

[7] While these events may indeed be beyond the consumer's control, their liability for the debts is based on their contractual agreements with the lenders.

[8] Thomas A. Durkin, Gregory Elliehausen, Michael E. Staten, and Todd J. Zywicki, *Consumer Credit and the American Economy*, New York: Oxford University Press, 2014, pp. 3-5

The number of CRAs grew exponentially over the years and began to extend to a wider range of creditors, including banks and other types of financial institutions. By the early-1970s, there were more than 2,250 CRAs nationwide.[9] Most were relatively small cooperatives that covered a limited geographic area and operated solely for the benefit of their members. They were typically industry-specific in their focus (e.g., retail, banking, etc.) and were often limited to reporting only negative information about their customers, be it a missed payment or something of a more dubious nature, for example, news of a recent divorce or arrest.[10]

As the decade progressed, however, the structure of the industry began to change, as did the nature of the data provided through credit reports. Triggered by rapid advances in computer technology, the emergence of interstate banking, and an explosion of unsecured credit, local and regional CRAs began to consolidate through a series of mergers and acquisitions in order to serve a broader array of lending activity across a wider range of geographic areas. Credit reports also began to provide a fuller and more objective picture of the consumer's credit profile, including the reporting of both positive and negative payment histories (sometimes referred to as "full file reporting").

There are three nationwide credit bureaus that dominate the credit reporting space today: Equifax, Experian and TransUnion. In addition to the provision of credit reports,[11] each of these companies engages in data aggregation and other kinds of activities that fall both within and beyond the scope of the FCRA. There also continue to be a number of more specialized CRAs that are governed by the FCRA,[12] for example, companies that focus on specific types of credit (e.g., payday loans, utility and telecom payments, etc.) or on other kinds of data that are used in various FCRA-covered transactions (e.g., residential and employment history, checking account use, etc.). However, the three nationwide credit bureaus—which are publically-traded companies with operations throughout the world and a combined market cap of roughly $46 billion[13]—represent the cornerstone of the U.S. credit reporting system today.

The use of credit reports has also changed over time with advances in technology and enhanced analytics. Traditionally, creditors had to evaluate a consumer's creditworthiness by examining the numerous trade lines and other information contained in their credit file. While there were broad guidelines for this assessment—for example, no more than a certain number of missed payments over a certain period of time—this manual process was time-consuming, error-prone and inherently subjective. This began to change with the emergence

---

[9] CFPB, op. cit., p.7

[10] Mark Furletti, "An Overview and History of Credit Reporting," Payment Cards Center Discussion Paper, Federal Reserve Bank of Philadelphia, June 2002, pp 3-5. https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2002/CreditReportingHistory_062002.pdf

[11] While similar in content, the credit reports provided by the nationwide credit bureaus differ somewhat due to differences in coverage and data reporting cycles.

[12] CFPB, op. cit., p.7

[13] Based on share prices on November 9, 2018.

of statistical tools known as "credit scores."[14] The first credit scores were developed by William Fair and Earl Isaac in the late-1950s, and branded as "FICO® Score".[15] Initially, credit scores were used almost exclusively by retailers. However, as banks' issuances of unsecured credit cards began to explode, so did their use of credit scores. The widespread adoption of credit scores became a reality in the early-1990s when Freddie Mac and Fannie Mae made them part of their underwriting requirements and automated underwriting systems (AUS), and, in the process, extended their use to the mortgage market.

There are numerous credit scores and credit score providers in the market today, often targeted for specific uses, populations and industries. For example, there are two major multi-purpose (or generic) credit scores: the FICO® Score and the VantageScore®.[16] Each has gone through a number of iterations, and older versions are still in use today. There are also numerous specialized scores that are developed and marketed for specific purposes. Some are designed for new accounts or business credit cards. Others are geared to specific industries, for example, retail credit cards, automobile loans, mortgages and insurance. While generic credit scores are designed to capture a consumer's performance on any kind of trade line, these more specialized credit scores rank-order consumers based on their expected performance on a specific type of credit (e.g., car loan) over a specified period of time.

The widespread adoption of credit scores and automated underwriting has clearly made the lending process more efficient by reducing the need to do intensive, line-by-line reviews of the numerous items that appear in a consumer's credit report. By relating these various line items to the consumer's subsequent performance on different forms of debt (e.g., the presence of a 90-day delinquency), credit scores provide a simple, statistically-based measure of a consumer's willingness and ability to handle their financial obligations. Indeed, according to one survey, most lenders now rely on credit scores, as opposed to the credit report itself, as an input to their credit decisions.[17]

Research has also found that the use of credit scores has led to more objective—and ultimately fairer—lending decisions. For example, a Freddie Mac study examined the original loan application files for a sample of mortgages purchased through one of its special affordable housing programs, and used these files to compare the results of manual underwriting to the use of credit scores and automated underwriting.[18] The study not only

---

[14] David A. Price, "Credit Scoring and the Revolution in Debt," *Econ Focus*, Vol. 17(4) (2013): 26-27. https://www.richmondfed.org/-/media/richmondfedorg/publications/research/econ_focus/2013/q4/pdf/full_issue.pdf
[15] FICO® Score is a registered trademark of FICO.
[16] VantageScore® scores are based on models produced by VantageScore Solutions, LLC, which is a joint venture of the three national credit bureaus. FICO® scores are based on models produced by FICO. Both score brands are distributed through the nationwide credit bureaus.
[17] Adi Osovsky, "The Misconception of the Consumer as a Homo Economicus: A Behavioral-Economic Approach to Consumer Protection in the Credit-Reporting System" *Suffolk University Law Review*, 46 (3) Volume 46, Issue 3, 2013. suffolklawreview.org/wp-content/uploads/2014/01/Osovsky_Lead.pdf
[18] Susan Wharton Gates, Vanessa Gail Perry, and Peter M. Zorn, "Automated Underwriting in Mortgage Lending: Good News for the Underserved?" *Housing Policy Debate*, Volume 13, Issue 2, 2002. https://www.researchgate.net/publication/239749502_Automated_underwriting_in_mortgage_lending_Good_news_for_the_underserved

found that automated underwriting did a better job in predicting future defaults; it also concluded that the resulting increase in accuracy would lead to higher approval rates, particularly for minority borrowers. These and other results led a 2007 Federal Reserve report to endorse the use of credit scores, concluding that: "by providing a low-cost, accurate, and standardized metric of credit risk for a pool of loans, credit scoring has broadened creditors' access to capital markets, reduced funding costs, and strengthened public and private scrutiny of lending activities."[19]

One thing that has not changed about the basic structure of the credit reporting industry is the voluntary nature of its data collection efforts. While creditors are encouraged to report on the payment histories of their customers, there is no regulatory or legal requirement that they do so. The fact that credit reporting is voluntary also means that there is no requirement that a credit file include all information about a consumer's credit activity or behavior. For example, the three nationwide credit bureaus use a standardized format and list of data elements for data furnishers, created by the Consumer Data Industry Association (CDIA), known as Metro2. While some fields are mandatory (e.g., credit limit, outstanding balance, minimum payment), others are requested, but not required (e.g., actual payment). As a result, because credit card issuers are often reluctant to report a consumer's actual (as opposed to required) monthly payments in order to protect their better accounts from potential "poaching," it is difficult to distinguish between consumers who pay off their balances every month ("transactors") from those who only pay the minimum amount that is due ("revolvers").

In the past, many CRAs enforced a reciprocal policy (sometimes known as "give-to-get") that required creditors and other potential users seeking information on a particular consumer to provide information on their entire customer base—a policy which ensured that entities "who benefit from a credit reporting company's competitive intelligence are themselves exposed to the same data reporting efforts as their peers."[20] However, none of the nationwide credit bureaus enforce this practice today. Instead, the primary reason that larger creditors are willing to share their data is that they recognize that if they do not contribute, their competitors would likely follow suit, thereby reducing the value of a common resource.[21] A second reason that creditors are willing to furnish information on their accounts is to improve the performance of their own portfolios. In the absence of widespread credit reporting, there would be little, if any negative consequences to borrowers who are consistently late on their payments or otherwise fail to meet their financial obligations because they could always go to another lender.

The inherent value of the data contained in consumers' credit reports to financial institutions is evidenced by the widespread reporting of the data. In 2012, the three nationwide credit bureaus maintained credit files on over 200 million adults and received information from

---

[19] Board of Governors of the Federal Reserve System, "Report to Congress on Credit Scoring and its Effects of the Availability and Affordability of Credit," August 2007. p. S-4.
https://www.federalreserve.gov/boarddocs/rptcongress/creditscore/creditscore.pdf
[20] Furletti, op. cit., p. 8
[21] CFPB, op. cit., p. 15

approximately 10,000 furnishers of data.[22] On a monthly basis, these data furnishers provided information on over 1.3 billion consumer credit accounts and other trade lines, with roughly sixty percent coming from retail- and network-branded revolving credit cards. The reporting of these data is highly concentrated among a few large institutions, primarily banks, with the ten largest data furnishers accounting for more than half of all reported accounts.

2.2 The Role and Impact of Credit Bureaus

Credit bureaus were formed in order to mitigate the risk that is inherent in any credit decision, namely, that the borrower will know more about their own ability and willingness to repay a financial obligation than any individual creditor is likely to know (often referred to as "information asymmetry").[23] This remains their primary purpose today. By providing an objective, comprehensive view of the consumer's use of credit, the information contained in a consumer's credit file enables potential creditors to make better lending decisions, which in turn leads to lower rates of default and enables creditors to serve a wider range of potential customers at a lower cost. The net result is greater access to credit for consumers and more robust economic growth.

One study summed up the benefits of comprehensive credit reporting as follows:[24]

- *Preventing delinquencies and defaults* by giving lenders a better understanding of their risk and by incenting consumers to make good on their obligations (e.g., reducing "moral hazard");

- *Enhancing competition* by reducing the barriers to entry that would otherwise occur if credit data were costly to obtain or if it were only available to existing market participants;

- *Increased mobility of both labor and capital* by making "credit reputations" portable and by enabling the development of a secondary market for various types of credit; and

- *Ensuring credit availability and economic resiliency* by giving lenders the information they need to assess the risk of potential new borrowers and to design and price products to meet the needs of previously underserved populations.

The benefits that flow from comprehensive credit reporting are not just theoretical. Indeed, they have been demonstrated by numerous academic studies, many of which are based on cross-country comparisons of different credit reporting regimes. For example, a recent World Bank study found that consumers in countries where CRAs cover a higher share of the adult

---

[22] Ibid. p. 3
[23] For a fuller discussion, see Durkin, et al., op. cit., pp. 241-286; Daniel B. Klein, "Credit-Information Reporting: Why Free Speech Is Vital to Social Accountability and Consumer Opportunity", *The Independent Review*, Vol. 5(3) (Winter 2001): 325-344. http://www.independent.org/pdf/tir/tir_05_3_klein.pdf
[24] Durkin, et al., op. cit., pp. 266-273

population have greater access to credit cards and consumer loans, and that private sector lending accounts for a larger share of the overall economy.[25] It also found that credit reporting systems that include credit history data from sources in addition to banks—for example, retailers, finance companies and utility companies—cover a broader range of consumers. Likewise, simulations based on U.S. data suggest that including positive as well as negative information in a consumer's credit report "can lead to significant increases in *both* the availability of credit and the likelihood that loans are repaid."[26]

While a number of factors could be at work, the maturation of the U.S. credit reporting system—combined with the development and widespread use of credit scores and the emergence of interstate banking—has certainly been accompanied by a dramatic increase in consumers' use of credit, particularly credit cards.[27] For example, in 1956 about fifty-five percent of U.S. households had a mortgage or some other form of installment debt. By 1998, this figure had risen to seventy-five percent, representing some 29.7 million additional households. The story was much the same for credit cards, but more dramatic. Between 1983 and 1998, the percentage of households with at least one general purpose credit card increased across all income categories, with the largest increases occurring at the lower deciles of the income scale. Within this twelve-year period, the total number of households with at least one credit card increased by more than 25 million.

Beyond their basic function of facilitating consumer credit, there are other important roles that credit bureaus play that set them apart from most other large-scale data aggregators. In order to ensure the accuracy of the data that they collect and distribute, credit bureaus must verify that the information that is supplied by a particular creditor is assigned to the right consumer; for example, that the Jim Smith who recently took out a mortgage from United Bank is the same Jim Smith who recently paid his Mastercard bill from Chase.[28] Credit bureaus also conduct regular checks on their entire database to remove duplicate or incomplete files, and to ensure that the files do not contain information on more than one person. Finally, credit bureaus coordinate the process through which consumers are able to challenge the accuracy of their credit report with the entity that provided the specific data. In doing so, credit bureaus essentially perform the role of a "trusted orchestrator" that assembles and coordinates various data items obtained from numerous public and private sources.

3.0 The Current Legal and Regulatory Regime

The regulatory and legislative framework that is in place for credit bureaus today addresses the three basic issues that underlie the current privacy debate: consumer consent, acceptable use, and data security. Its key elements can be found in the Fair Credit Reporting Act

---

[25] World Bank Group, "Getting Credit: Credit Information, Casting a wide net to expand financial inclusion" *Doing Business 2017*, p. 59. www.doingbusiness.org/.../DB17-CS-Getting-credit-information.pdf
[26] Durkin, et. al., op. cit., p. 266
[27] John M. Barron and Michael E. Staten, "The Value of Comprehensive Credit Reports", in *Credit Reporting Systems and the International Economy*, edited by Margaret J. Miller, Boston: MIT Press, 2003, pp. 282-3
[28] For a detailed discussion of the processes used to ensure the accuracy of the data, see CFPB, 2012, op. cit., pp. 18-22

(FCRA), along with certain provisions contained in the Gramm-Leach-Bliley Act (GLBA)[29] and the Equal Credit Opportunity Act (ECOA).[30] Other provisions in the ECOA, as well as the Fair Housing Act, Title VI of the Civil Rights Acts, and other antidiscrimination laws, also place important restrictions on the kinds of personal data that can be used for specific purposes, including those that are subject to the FCRA.[31] While credit bureaus remain subject to enforcement action by the Federal Trade Commission (FTC) under the Unfair or Deceptive Practices Act (UDAP), since 2013 the Consumer Financial Protection Bureau (CFPB)[32] has held a supervisory role with authority to examine, investigate and impose penalties pursuant to the various more expansive Unfair, Deceptive or Abusive Acts or Practices (UDAAP) laws,[33] as well as the FCRA, the GLBA, and other laws.

The sharing of objective information on a consumer's financial track record is critical to the basic role that credit bureaus perform. As a result, with only a few exceptions, the imposition of broad privacy concepts such as "opting in" or "opting out"—or the "right to be forgotten"—simply do not apply and are not part of the FCRA.[34] If consumers were allowed to pick and choose the information that is contained in their credit reports, the validity of those reports would quickly disappear, along with the numerous benefits that credit bureaus currently provide. There are also legitimate questions about who actually owns the data—the consumer or the entity that is reporting their experience with the consumer. For these reasons, privacy regimes such as the GDPR and California' Consumer Privacy Act have explicit carve-outs for credit reporting agencies. In fact, with only a few exceptions, the FCRA (as amended) explicitly prohibits states from enacting statutes that override its key provisions.[35]

3.1 Key Provisions

The FCRA is designed to allow the sharing of critical personal financial data while ensuring consumer privacy by strictly limiting the permissible uses of the data. Its provisions apply to any entity that either provides or uses data related to credit, employment, insurance or

---

[29] GLBA provisions include the so-called safeguards rule, which requires "financial institutions" to safeguard personally identifiable financial information (PIFI) about customers by assessing risk to PIFI and developing a plan. The FTC has determined that the rule applies to CRAs.

[30] These ECOA provisions primarily relate to consumer privacy and the sharing and use of sensitive financial data, including adverse action notifications.

[31] Hereafter, provisions of the ECOA that relate to adverse action notifications are considered as included when we cite the FCRA as it relates to the use of protected consumer information.

[32] While the official name of the agency is the Bureau of Consumer Financial Protection (CFPB), its current director has indicated that the Bureau will keep the logo "CFPB" except for legal filings, reports, and official business. *See* https://www.politico.com/story/2018/12/19/kraninger-consumer-financial-protection-bureau-1069173

[33] UDAAP laws have been used by the FTC, CFPB and states attorney generals to impose sanctions and penalties for failure to secure the data.

[34] Consumers do have the right to "opt out" of the use of their files for marketing purposes, and to freeze their files so that they cannot be used for future offers of credit until the consumer removes the freeze from the file. However, they cannot opt-out of the collection of their credit history.

[35] See Durkin, et al., op. cit., p.254

housing decisions. Unlike the GDPR, the FCRA addresses issues of consumer privacy by imposing tight restrictions on who can access the data and how it can be used, rather than by stipulating the specific types of data that can be collected or by imposing specific requirements for consumer consent. (See Table 1.) In order to access a consumer's credit file, data users must identify the specific way in which the data will be used and limit its use to a single application (i.e., no "double dipping") to ensure the data's proper use.[36]

Table 1: FCRA Requirements for Acceptable Use

User	Acceptable Use or Purpose
Creditors	• Underwriting applicants • Make "firm" offers of credit • On-going monitoring for risk exposure
Insurers	• Underwriting applicants • Making "firm" offers of insurance • On-going monitoring for risk exposure
Collection Agencies	• Resolving delinquent accounts, tax liens, foreclosures
Employers	• Background checks (explicit written consent required)
Landlords, telecom companies, utilities	• Background checks on prospective tenants or customers
Financial Regulators	• Safety and soundness monitoring
Government Agencies	• Eligibility determination for certain purposes

Source: FCRA, §604 (a)

The FCRA also ensures the transparency and accuracy of credit reports by giving consumers a series of rights, including the right to access their files and the ability to dispute inaccurate information.[37] (See Table 2.) These rights were further enhanced by recent legislation that allows consumers to "freeze" their credit files for no additional fee; while their files are still available for certain purposes—for example, ongoing account reviews and collections—this enables consumers to protect their data from potentially fraudulent uses. Under FCRA, "consent" to access a consumer's credit file is implied by a request for credit or insurance[38] or by the receipt of a firm credit offer. Once credit is granted, that implicit consent applies as long as the contract between the lender and the borrower is in force. Explicit "consent" is only required for employment inquiries or when the consumer grants access to someone for a purpose that would not otherwise be considered a permissible use (e.g., credit counseling).

---

[36] See Federal Trade Commission, "Background checks? Don't double-dip", *Business Blogs,* February 2017, available at https://www.ftc.gov/news-events/blogs/business-blog/2017/02/background-checks-dont-double-dip.
[37] Consumer Financial Protection Bureau, "A Summary of Your Rights Under the Fair Credit Reporting Act", April 2015. https://files.consumerfinance.gov/f/201504_cfpb_summary_your_rights-under-fcra.pdf. Recent legislation, the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 also gave consumers the right to a free credit freeze. See https://www.ftc.gov/news-events/press-releases/2018/09/starting-today-new-law-allows-consumers-place-free-credit-freezes
[38]Vermont is the one exception, whose state law was grandfathered in and requires residents of that state to give explicit consent for pulling credit inquiries.

Table 2: Key Consumer Rights

Objective	Provision

Transparency	• Creditors, employers and insurers who deny an application based on a consumer's credit file must notify the applicant and identify information source
	• Consumers have the right to request and obtain all information contained in their credit file. They also have the right for one free credit report each year, or if they are:
	    ○ subject to an adverse action based on their credit file
	    ○ the victim of identity theft or fraud
	    ○ receiving public assistance, or
	    ○ unemployed but expecting to seek employment within 60 days
	• Consumers have the right to dispute incomplete or inaccurate information in files
	• Consumers have the right to request the placement of fraud alerts, extended fraud alerts, and active duty alerts

Accuracy	• CRAs are required to investigate disputed information with the data furnisher unless the dispute is frivolous, and to correct or delete any inaccurate information once resolved • Consumers have the right to add an explanatory statement to disputed items if they are not resolved
Privacy	• Access is strictly limited to parties with "permissible purpose" • Access by employers requires explicit consumer consent • Consumers have the right to limit prescreened offers of credit and insurance they get based on information in their credit report • Consumers have the right to "freeze" their credit file for free • In most cases, negative information must be deleted from credit file after seven years (or ten years old in the case of bankruptcies)

Source: CFBP, 2015

Importantly, the FCRA does *not* allow consumers to "pick and choose" the specific trade lines that they want to be reported, nor does it give them the general right to be "forgotten." Doing so would undermine the ability of credit bureaus to provide an accurate and comprehensive picture of the consumer's financial situation, which in turn would lead to inappropriate lending decisions and ultimately harm consumers and creditors alike. However, the FCRA does allow for something akin to a "right be forgiven" by requiring credit bureaus to delete most derogatory information after seven years and, in the case of personal bankruptcies, after ten years. This reflects a value judgment on the part of policy makers that individuals who amend their ways and pay their bills on time should not be penalized for something that occurred in the relatively distant past.

The basic provisions of the FCRA are not just applicable to credit bureaus. They also apply to other credit reporting agencies, defined as any entity "which for monetary fees, dues or on cooperative nonprofit basis regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information for the purpose of furnishing

consumer reports to third parties."[39] Thus, the FCRA provisions would still apply even if the structure of the industry changes. For example, if entities such as Facebook, Amazon or Google begin to use or provide their proprietary data as inputs to the kinds of activities that are currently covered by the FCRA, they would be subject to the same data validation and reporting requirements that apply to credit bureaus.[40] Moreover, once the data is used in a FCRA-covered activity, it is always subject to these requirements, including limitations related to its use. While there is always room for improvement, the overarching legal and regulatory framework that is in place for credit bureaus today can and should provide the basic guardrails going forward, regardless of how the industry ultimately evolves.

3.2 Data Security

One area on which the FCRA is relatively silent relates to data security. While a patchwork of data security laws are emerging at the state and local levels, "there is no universal federal law on data security, and jurisdiction is shared among regulators that oversee banks, nonbank financial services companies and nonfinancial companies."[41] A recent Treasury report summarized the current situation of credit bureaus as follows:

> "While the credit bureaus are subject to state and federal regulation for consumer protection purposes, and have been subject to state and federal enforcement actions related to data security, they are not routinely supervised for compliance with the federal data security requirements of the Gramm-Leach-Bliley Act."[42]

The net result is regulatory confusion and disagreement over the specific data security principles, standards and processes that should apply to credit bureaus, despite the highly sensitive nature of the data contained in consumers' credit files.

The FTC's Safeguards Rule, which implements sections of the GLBA, establishes data security standards for regulated financial institutions that are under its jurisdiction, including credit bureaus.[43] However, this framework is very broad and offers little, if any specific guidance on what is required to meet those standards. The CFPB has also acted as a data security regulator under its UDAAP authority, despite the lack of specific guidance on the standards it expects companies to follow. Up until now, what guidance there is has typically been provided through enforcement actions or litigation, an approach that is sometimes known as "regulation by enforcement." While the former CFPB Director, Mick Mulvaney,

---

[39] 15 U.S. Code § 1681a

[40] Jennifer Archie, Kevin Boyle and Kelsey McPherson, "Aggregator of Social Media Info Subject to FCRA", June 15, 2012. https://www.globalprivacyblog.com/privacy/social-media-info/

[41] Michael Gordon, Elijah Alper and Leah Schloss, "The CFPB and Data Security Enforcement," *BNA Insights*, June 8, 2016. https://www.bna.com/bna-insights-cfpb-n57982073820/

[42] U.S. Treasury, op. cit., p.12

[43] For provisions specifically applying to credit bureaus, see 16 CFR 314 - Standards for Safeguarding Customer Information, January 1, 2009. https://www.gpo.gov/fdsys/pkg/CFR-2009-title16-vol1/pdf/CFR-2009-title16-vol1-part314.pdf

announced his intention to issue guidance on what constitutes an "abusive practice,"[44] whether this will occur under his replacement remains unclear.

The recent Equifax settlement with the California Department of Business Oversight and seven other state regulatory agencies highlights the uncertainties that currently exist with respect to the specific data security standards that should be applied to credit bureaus.[45] Under this action, rather than applying the FTC's Safeguard rule—which is very broad—the states chose to apply the more detailed Interagency Guidelines that were developed by federal banking agencies and the Federal Financial Institutions Examination Council (FFEIC) pursuant to the GLBA. While many aspects of these guidelines are appropriate for credit bureaus, they are specifically designed for banks, and do not necessarily reflect the risks that are specific to CRAs.

In the future, there may well be technical solutions to issues related to data security. For example, something akin to block chain or distributed ledger technology could conceivably be used to guarantee secure transactions and data exchanges. Another frequently mentioned alternative would be to replace static identifiers such as social security numbers or biometric data—which can never be changed—with some form of short-lived, multifaceted authentication process. Under such an approach, once the identity of the consumer is verified by a neutral party to the exchange, IDs could be easily changed and remain unknown to both the data furnisher and the data user. Thus, while hackers might still be able to slip through the door, they would be unable to link the data to any specific individual, greatly limiting its value and potential use.

However, because even the best technologies will inevitably become obsolete, there is a clear need for national data security standards that specify the processes and procedures that companies must follow in order to protect a consumer's data, rather than the specific technical approaches that should be employed. In developing these standards, policy makers should consider the fluidity and ever-evolving nature of technology. Such standards must be clear and certain to the regulated entities, appropriate to the risks involved, and sufficiently detailed to be understood and auditable for compliance purposes. Under such a regime, compliance would be based on a company's adherence to all applicable standards, rather than on the incidence of a data breach. Similarly, any penalties would be based on failure to comply with the standards and not automatically imposed if a data breach occurs. Data security standards should also clarify the specific obligations of the data aggregator to the consumer in the event of a data breach. While all fifty states have enacted security breach

---

[44] Mike Sorohan, "Mulvaney: Regulation by Enforcement is Done," *MBA NewsLink*, October 16, 2018. https://www.mba.org/mba-newslinks/2018/october/mba-newslink-tuesdayam-10-16-18/mulvaney-regulation-by-enforcement-is-done

[45] Equifax Consent Order, June 25, 2018. https://dbf.georgia.gov/sites/dbf.georgia.gov/files/related_files/press_release/Equifax-Final-Consent-Order_6-25-18.pdf

notification laws, their standards differ with respect to the requirement for consumer harm, the form of the data breach, and the specific notification requirements.[46]

In the event that Congress fails to enact national data security standards, the FTC and CFPB should work together to develop more detailed data security guidance for credit bureaus. This would be consistent with the Treasury's recent recommendation that "the relevant agencies use appropriate authorities to coordinate regulatory actions to protect consumer data held by credit reporting agencies."[47] Treasury also recommended that "Congress continue to assess whether further authority is needed in this area,"[48] an assessment that should include the possibility of granting the FTC (or other appropriate federal agency) the authority to routinely monitor credit bureaus for compliance with applicable data security standards. The guidance that would result from routine compliance reviews would go a long way towards clarifying what constitutes "best practices" with respect to the protection of credit bureau data, and ideally reduce, if not eliminate the practice of "regulation by enforcement."

3.3 Data Accuracy

The accuracy of credit report data has also been a subject of considerable debate over the years. There are many potential sources of errors in a consumer's credit report.[49] Examples of errors include when a consumer enters inaccurate information in their application for credit, or when a data furnisher sends inaccurate, incomplete or outdated information to the credit bureau. Errors can also occur when a credit bureau does not have sufficient data to match a credit report to the right individual, when delinquent accounts are transferred to collection agencies, or when consumers become victims of identity theft. Some of these inaccuracies may be relatively minor (e.g., an incorrect or outdated address) and have little, if any impact on the consumer's credit score or ability to obtain a loan. However, others can be more significant, for example, a reported collection that has been assigned to the wrong John Doe.

The FCRA requires data furnishers to "establish and implement reasonable written policies and procedures regarding the accuracy and the integrity of the information" provided to credit bureaus, and to "promote… [the] conduct [of] reasonable investigations of consumer disputes."[50] This latter requirement was bolstered by a 2013 CFPB bulletin warning data furnishers that they will face potential disciplinary action if they do not properly review the information submitted to credit bureaus in conjunction with consumer disputes, as well as by CFPB enforcement actions against American Express for the way that it handled disputes directly received from consumers.[51] The FCRA also requires credit bureaus to ensure the

---

[46] National Conference of State Legislators, "Security Breach Notification Laws," September 29, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[47] U.S. Treasury, op. cit., p.12

[48] Ibid, p.12

[49] CFPB, op. cit., pp. 24-26

[50] See 12 C.F.R. § 1022.42 and 12 C.F.R. pt. 1022, App. E.

[51] See Andrew M. Smith and Ana-Maria Ignat, "Brave New World for Data Furnishers" *Law360*, September 24, 2013. https://media2.mofo.com/documents/130917-brave-new-world-for-data-furnishers.pdf

maximum possible accuracy and to have processes to monitor data furnishers for patterns or practices that indicate inaccuracy. For example, up until recently, consumer credit reports contained information on tax liens and civil judgments, which were a frequent source of errors due to difficulties in linking these public records data to the right consumer. As a result, all three bureaus have stopped reporting on these items.[52] However, while credit bureaus have a clear financial incentive to ensure that credit reports are as accurate as possible in order to increase the value of their data, they are simply not in a position to validate every line item that is contained in an individual's credit file.

As a result, the FCRA puts the consumer squarely in the driver's seat in determining the accuracy and completeness of their credit report. Some have questioned whether consumers are up to this task. As one skeptic put it:

> "FCRA envisions rational and vigilant consumers, and imposes various monitoring responsibilities on those consumers. However, research in behavioral economics demonstrates how consumers' decision-making processes can be irrational because they are biased by numerous judgment errors."[53]

Many consumers simply do not take the time to review their credit reports unless they are turned down for a loan, a victim of identity theft, or encounter some other sort of problem. Many do not have the expertise to identity and dispute errors that could have a significant impact on their credit scores. Some may perceive accurate information to be inaccurate (for example, a joint account that was assigned to one spouse in a divorce settlement is accurately reported in both files, even though the divorce makes it one person's responsibility). And few, if any, are motivated to correct an error that ultimately works in their favor (for example, a well-performing loan that is in a consumer's file that actually belongs to someone else). For these reasons, the incidence of errors cannot be judged based on the number of disputes that are submitted to credit bureaus, which are initiated by consumers, not always valid, and often reported multiple times.

While there have been several attempts to estimate the incidence and significance of reporting errors, their finding are inconsistent.[54] For example, one industry-funded study estimated that about 19% of all credit reports contained some kind of error, but less than one percent of all reports had "serious" errors that would change an individual's credit score by more than twenty-five points.[55] Another study by the FTC found a similar overall error rate (twenty-one percent) but concluded that the incidence of "serious errors" was about five

---

[52] Penny Crossman, "Will dropping tax lien data from credit reporting lead to bad loans?" *American Banker*, April 02 2018. https://www.americanbanker.com/news/will-dropping-tax-lien-data-from-credit-reporting-lead-to-bad-loans

[53] A. Osovsky, op. cit., p.933

[54] For a thorough review of these and other related studies, see Durkin, et. al., pp. 273-286.

[55] Michael A. Turner, Robin Varghese, and Patrick D. Walker, "US Consumer Credit Reports: Measuring Accuracy and Dispute Impacts", Policy and Economic Research Council, May 2011. https://www.transunion.com/docs/rev/aboutTransunion/credit-studies/Efficacy_DQreport.pdf

percent.[56] While it is difficult to determine the reasons for these discrepancies, one possible explanation is that the FTC study used experts to assist consumers in reviewing their reports, while the industry study did not. But even if one could agree upon the underlying incidence of serious errors, such errors—whether positive or negative—have different implications for different consumers. For example, a twenty-five point decrease in a consumer's credit score would have little, if any impact on consumers with relatively high existing scores (e.g., mid-700s), while the impact on consumers whose scores are relatively low (e.g., mid-600s) would be far more consequential. As one reviewer put it, "in truth, no one really knows exactly how many people are affected by credit report errors."[57]

The question for policy makers ultimately boils down to how much additional accuracy they are willing to buy.[58] While further regulatory requirements could be imposed on data furnishers and credit bureaus, the costs associated with these requirements would be relatively high and ultimately be borne by consumers. And if the requirements proved to be too cumbersome, such policies could threaten the overall scope and coverage of credit reports given the voluntary nature of the reporting system. Some countries have established public credit bureaus under the assumption that the government can do a better job in ensuring the collection and the accuracy of the data; however, research has consistently found that private credit bureaus are more efficient and effective.[59]

Understanding that it is impossible to completely eliminate errors, the focus from both U.S. regulators and credit bureaus has instead been on facilitating consumers' access to their credit reports and making redress easier, which was the primary objective of the 1996 and 2003 amendments to FCRA. There is always room for improvement, particularly with respect to the need for better consumer education and counseling. For example, certain aspects of the Credit Repair Organizations Act (CROA), which was designed to protect consumers from so-called "credit doctors," are limiting the ability of credit bureaus to provide certain services in this space. As a result, the Treasury has recommended that "Congress amend the [CROA] to exclude national credit bureaus and national credit scorers in order to allow these entities to provide credit education and counseling services to consumers to prospectively improve their credit scores."[60] While these and other efforts to empower consumers should be supported, the FCRA's basic approach for balancing concerns over data accuracy with the efficiency and scope of credit reporting remains appropriate today.

4.0 The Future Role of Credit Bureaus

---

[56] Federal Trade Commission, "Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003", December 2012. https://www.ftc.gov/reports/section-319-fair-accurate-credit-transactions-act-2003-fifth-interim-federal-trade

[57] Michael Osakwe , "How Common are Credit Report Errors?" April 21, 2016. https://www.nextadvisor.com/blog/credit-report-errors

[58] Michael E. Staten and Fred H. Cate, "Accuracy in Credit Reporting", in *Building Assets, Building Credit*, edited by N. Retsinas and E. Belsky, Brookings Institution, 2003, p. 262

[59] For example, see OECD, "Facilitating Access to Finance: Discussion Paper on Credit Information Sharing," Undated. http://www.oecd.org/global-relations/45370071.pdf

[60] U.S. Treasury, op. cit., p. 12

The vast amount of personal data that is currently available from large scale data aggregators—and the growing use of such data for the development and application of a wide variety of behavioral models, including credit scoring—has led some to question whether credit bureaus are becoming obsolete.[61] The answer to this question in large part depends on the extent to which such data ultimately provides a better way of measuring credit risk. It also depends on the degree to which the credit bureaus' current role as a trusted broker of consumer data is no longer valued in financial transactions.

This section examines three closely related trends that are affecting credit bureaus and the credit reporting industry. It begins by examining the extent to which different types of "alternative" data could be used to augment or even replace the information now contained in consumers' credit reports. It then explores broader issues related to the increasingly sophisticated analytic tools that are affecting virtually every aspect of modern life, including the assessment of a consumer's creditworthiness. Finally, it examines the rise of Fintechs and mobile payment apps, and the extent to which this trend could undermine the inherent value of credit reports and, hence, credit bureaus.

4.1 The Use of Alternative Data

One of the major trends affecting credit bureaus today is the increasing demand for alternative data not typically included in a consumer's credit report. Roughly ninety percent of all consumers over eighteen years of age have credit files at one or more of the credit bureaus. At the same time, however, some 26 million consumers do not have credit files, and another 20 million have files that are either "too thin" or "too old" to receive a traditional credit score.[62] These 46 million so-called "credit invisibles"—who are disproportionately black or Hispanic and who are more likely to live in low income neighborhoods—are often caught in a vicious circle where their current lack of credit makes it virtually impossible to qualify for credit going forward.

The desire to broaden consumers' access to a wider range of financial services has led many to call for the development of alternative credit scores based in whole or in part on data not typically found in a standard credit report. Such "alternative" data, which could be used to augment or even replace traditional credit bureau data, fall into three broadly-defined categories:

---

[61] For example, see Robin Raskin, "Rethinking Credit Scores in the Age of Fintech," Huffington Post, October 4, 2017. https://www.huffingtonpost.com/entry/rethinking-credit-scores-in-the-age-of-fintech_us_59d3c16ce4b02508a0a07a4b

[62] Kenneth P. Brevoort, Philipp Grimm, and Michelle Kambara, *Data Point: Credit Invisibles*. Consumer Financial Protection Bureau, May 2015. http://files.consumerfinance.gov/f/201505_cfpb_datapoint-credit-invisibles.pdf

- *"credit proxies"* which measure a consumer's performance on their other important financial obligations, for example, their monthly rent, utility, and telecom payments;

- *"banking data"* which include information drawn from the consumer's checking, savings, and money market accounts, for example, average monthly balances and average inflows and outflows; and

- *"non-financial personal data"* which could include a wide range of personal data harvested from a consumer's digital footprint, such as their social media likes and interests, their cell phone use, or even their shopping patterns.

While these various types of data have been shown to have some degree of predictive power, they differ in a number of important ways that make them unlikely to replace credit reports any time soon.

Credit Proxies

Credit proxies attempt to measure a consumer's credit worthiness by capturing their performance on other recurring financial obligations. The most commonly-accepted alternatives are based on the consumer's monthly rent, utility and telecom payments. However, other potential candidates could include insurance payments, performance on payday loans, or regular remittances to family members living abroad. While not strictly forms of credit, including a consumer's track record with respect to meeting at least some of these obligations has been shown to be an effective way of expanding access to credit, especially for consumers with thin or non-existent credit files.[63] For example, one study estimated that the inclusion of telecom and utility data in traditional scoring models would increase acceptance rates by about ten percent for the overall population, and by more than twenty percent for blacks, Hispanics, and consumers making less than $20,000 a year.[64] Other studies have found that the inclusion of rental payments would also have a significant and positive impact on consumers' access to credit.[65]

[63] For a review of these studies, see Rachel Schneider and Arjan Schutte. "The Predictive Value of Alternative Credit Scores," Center for Financial Services Innovation Report, November 2007. https://cfsinnovation.org/research/the-predictive-value-of-alternative-credit-scores/. While the inclusion of rent or utility payments was generally found to have positive impact on consumers' access to credit, the opposite was true for remittance payments. See CFPB, "Report on the Use of Remittance Histories in Credit Scoring", 2014. http://files.consumerfinance.gov/f/201407_cfpb_report_remittance-history-and-creditscoring.pdf.
[64] Michael A. Turner, Alyssa Stewart Lee, Ann B. Schnare, Robin Varghese, and Patrick D. Walker, "Give Credit Where Credit Is Due: Increasing Access to Affordable Mainstream Credit Using Alternative Data," Policy and Economic Research Council and the Brookings Institution Urban Markets Initiative Report. 2006. https://www.brookings.edu/research/give-credit-where-credit-is-due-increasing-access-to-affordable-mainstream-credit-using-alternative-data/
[65] See Experian, "Credit for Renting: The Impact of Positive Rent Reporting on Subsidized Housing Residents," Experian Rent Bureau White Paper. 2014. www.experian.com/.../experian-rentbureau-credit-for-rent-analysis.pdf; Scott M. Stringer, New York City Comptroller, "Making Rent Count: How NYC Tenants Can Lift Credit Scores and Save Money," October 2017. https://newsroom.transunion.com/transunion-analysis-finds-reporting-of-rental-payments-could-benefit-renters-in-just-one-month

But despite the demonstrated value of such data—particularly rent, utility and telecom payments—they are rarely reported to credit bureaus, and when they are, they are typically restricted to collections. According to FICO, only about two and one-half percent of credit files have utility or telecom data that contain both positive and negative payment history, while less than one percent of files have such information on rental payments.[66] While each of the credit bureaus has proprietary data bases that include at least some of these kinds of data—which when used for credit decisions are covered by the FCRA—they are not included in the consumer's standard credit report. Instead, the data are marketed separately and sometimes used to create "alternative" credit scores for consumers with little, if any credit history.[67]

One such alternative data base has been assembled by the National Consumer Telecom & Utilities Exchange (NCTUE®), which is owned and operated solely for the benefit of its members, including cable companies, telecoms, and energy utilities. According to its marketing materials, NCTUE now has payment data on roughly 225 million consumers with over 460 million reported trade lines. Cable, mobile telephone, and landline telephone represent the vast majority of reported trade lines. While it is difficult to estimate coverage rates, they appear to be relatively high for cable and cell phone providers, but relatively low for "traditional" public utilities such local telephone companies and energy providers.

A variety of factors could account for these apparent differences in reporting rates. To begin with, cable and cell phone providers are typically regional or national in scope, and are actively fighting for market share. In contrast, local telephone, gas and electricity providers face little, if any competition, and are required to serve their entire community; as a result, the costs of sharing their customer data—which would make them subject to FCRA requirements—most likely outweighs the expected benefits that might otherwise come from targeted marketing or other uses of the data. The lower reporting rates among local telephone and energy utilities may also reflect the existence of state and local privacy laws that either prevent or discourage the reporting of such data, as well as continued opposition by some community groups to make such data available. What these community groups fail to recognize is that negative payment data is already reported whenever an account goes to collection, and that the failure to report positive payment histories only serves to penalize consumers who consistently pay their bills on time.

Proposed legislation attempts to encourage the voluntary reporting of utility, telecom and rental data by amending the FCRA to clarify federal law with respect to the reporting of such information. The latest version of the bill, introduced in the 115th Congress—S. 3040, The

---

[66] FICO, "Truth Squad: Can Scoring Rental Data Vastly Improve Credit Access?" May 10, 2017. https://www.fico.com/blogs/risk-compliance/truth-squad-can-scoring-rental-data-vastly-improve-credit-access/
[67] For example, Equifax has partnered with the National Consumer Telecom and Utility Exchange (NCTUE), FICO and LexisNexis Risk Solutions to create FICO XD, a credit score specifically designed for consumers with thin credit files that incorporates data on telecom and utility payments.

Credit Access and Inclusion Act of 2018—was introduced in June 2018, and is similar to H.R. 435, which was passed by the House in 2017. The bill would amend the FCRA to "allow a person or the Secretary of Housing and Urban Development [to furnish]…information related to the performance of a consumer in making payments ... under a lease agreement with respect to a dwelling or ... pursuant to a contract for a utility or telecommunications service,"[68] subject to certain limitations applying to consumers under a payment plan. However, neither the House nor Senate bill explicitly pre-empts existing state or local laws that prevent the reporting of such data. Moreover, groups such as the National Consumer Law Center continue to oppose the bill, arguing that for some consumers, it is better to have no credit than bad credit.

While the proposed legislation is certainly a step in the right direction, for the reasons noted above, it remains unclear whether such legislation would be enough to encourage the widespread reporting of local utility and telephone company data. According to Ballard Spahr:

> "[The] reporting of individual consumer histories would not be mandatory, and thus landlords, utility companies, and telecommunications providers could choose to maintain the status quo and report nothing at all. It seems unlikely that individual landlords and smaller utility companies would find that the benefits of furnishing accurate information to consumer reporting agencies outweigh the costs and risks associated with FCRA."[69]

The highly dispersed ownership structure of rental housing certainly makes the collection of rental data particularly challenging. While a few large landlords currently report to credit bureaus, the vast majority of rental housing is owned by individuals or smaller providers which have little, if any incentive to share their data—and assume the responsibilities that such data sharing would bring. Some web apps have attempted to fill the gap by serving as intermediaries between consumers, their landlords, and the credit bureaus; however, use of such apps has been relatively limited to date. Thus, while the proposed legislation may help to remove reporting barriers for HUD-assisted housing—which is specifically cited in the legislation and accounts for about 10% of all rental units[70]—its potential impact on the private rental market remains unclear.

Bank Data

A second type of "alternative" data would draw on information obtained from the consumer's checking and savings accounts to augment or even replace traditional credit

---

[68] See https://www.govtrack.us/congress/bills/115/s3040

[69] Taylor R. Steinbacher, "Proposed Credit Reporting Changes Pass House with Mixed Reviews," *Consumer Finance Monitor*, Ballard Spahr, August 2018. https://www.consumerfinancemonitor.com/tag/credit-access-and-inclusion-act-of-2017/

[70] According to HUD, roughly 4.65 million households receive some form of HUD assistance, compared to a total number of occupied rental units of 43 million. https://www.huduser.gov/portal/datasets/assthsg.html and https://www.statista.com/statistics/187577/housing-units-occupied-by-renter-in-the-us-since-1975/

reports. Use of such data would enable one to construct broad indicators of a consumer's financial well-being, including average balances at the end of each month and average inflows and outflows. It would also enable one to evaluate the consumer's individual financial transactions, including their specific sources and uses of funds. While banking data has long been used as an input to the underwriting process—for example, mortgage lenders typically require copies of the consumer's recent bank statements—there is no central clearing house for bank account data and as a result, it is cumbersome to use. However, the digitalization and aggregation of banking data greatly expands its potential uses, including credit scoring.

Savings, checking and money market account data would undoubtedly provide a powerful predictor of a consumer's ability to manage their financial obligations. For example, combined with information on a consumer's outstanding debts, information on their average discretionary income at the end of the month would provide a clear indication of how much additional credit they could support, which in underwriting terms is known as the consumer's "capacity" to handle the loan. However, the inherent value of this information—as well as general privacy concerns—has made banks reluctant to share such data. While there are proprietary data sources that provide limited information on a consumer's use of their checking accounts—for example, the frequency of overdrafts—more general data sharing on banking accounts is the exception, not the rule.

This is beginning to change with the emergence of Fintechs offering a range of mobile financial services to consumers who are willing to give them access to their banking data. For example, Fannie Mae recently announced a pilot program, known as Single Source Verification (SSV), which allows lenders to validate a borrower's income, assets and employment with reports provided by approved data aggregators such as Finicity and FormFree. More significantly, FICO recently announced that it has partnered with Experian and Finicity to introduce a new credit score—the UltraFICO™ Score—that augments traditional credit reporting data with transactional information drawn from a consumer's banking account, including the age of the account, the frequency of activity, and evidence of savings (e.g., the average ratio of inflows to outflows).[71] Importantly, these and other applications of banking data rely on the consumer's express consent to use their bank data for a specific purpose, as well as the willingness of their bank to give the data aggregator access to their files.

The concept of open banking—which has just been introduced in the United Kingdom—could further expand such applications and potentially lead to a new era of data sharing, with profound implications for how individuals engage and consume financial services and how creditors manage and control their risk.[72] Open banking is a system that enables customers to share their financial data with other financial institutions through the use of application

---

[71] See https://www.fico.com/en/newsroom/experian-fico-and-finicity-launch-new-ultrafico-credit-score
[72] Rob Haslingden. "Open Banking: Creating a New Era of Data Sharing," Experian White Paper, 2017. https://www.experian.co.uk/assets/resources/white-papers/open-banking-whitepaper-2017.pdf

programming interfaces (APIs). The UK model, which requires banks to comply with a consumer's request to share their data, was designed to increase competition in a highly concentrated banking system. As a result, it may be far less applicable to the mix of community, regional, and national banks that exists in the United States. However, if the concept of open banking catches on in the United States, access to banking data would provide an invaluable source of objective financial data that would help complete a consumer's financial profile, which in turn would lead to better services and better outcomes for consumers and lenders alike. If this in fact occurs, use of such data will be subject to the FCRA and all its associated requirements, whether that data becomes part of the consumer's traditional credit report or distributed on a one-off basis through separate channels.

Some observers have argued that opening up banking data to a broader array of uses, including credit scoring, poses a threat to consumer privacy and the security of their data. According to Sheila Bair, a former commissioner of the Federal Deposit Insurance Corporation (FDIC):

> "If the credit bureaus want to start routinely accessing our bank accounts, they should be subject to bank-like regulation. I've been a critic of big U.S. banks in certain areas, but I do believe their information security systems are substantially superior to the credit bureaus and that is due, in large part, to their regulated status."[73]

A representative of the Center for Financial Services Innovation agreed with this assessment, noting that: "We're getting to where we have larger sets of data housed in institutions that the entire financial services industry rests on, and they don't have the same regulation and security protocols a regulated bank would have,"[74] adding that the CFPB focuses more on consumer protection and less on the safeguards that need to be put in place to guard against a potential breach. Such comments underscore the conclusions reached earlier in this report that the data security standards currently applicable to credit bureaus need to be more explicit, and that adherence to these standards should be subject to routine compliance reviews by regulators.

Non-financial Personal Data

The third—and potentially most controversial—kind of "alternative" data includes a wide variety of non-financial personal data that can be harvested from a consumer's digital footprint (e.g., social networking, on-line purchases, web searches, etc.), their cell phone use (e.g., type of device, time and volume of calls, etc.) or even through the administration of so-called "psychometric" questionnaires.[75] Some of these data have been shown to be related to

---

[73] Penny Crosman, "New UltraFICO score stokes concerns about data privacy," *American Banker*, October 25, 2018. https://www.americanbanker.com/news/new-ultrafico-score-stokes-concerns-about-data-privacy
[74] Ibid.
[75] Entrepreneurial Finance Lab, "Alternative Credit Scoring in Emerging Markets," January 7, 2015. https://www.eflglobal.com/alternative-credit-scoring-emerging-markets

credit risk.[76] For example, studies have found that iOS users are generally better credit risks than Android users, as are consumers who applied for credit late at night as opposed to at other times of the day. Likewise, consumers with email addresses that use their name appear to be less risky than consumers whose email addresses are obscure. These types of non-traditional data are now being considered as alternatives to traditional credit reports in emerging markets where credit reporting is limited or non-existent. However, in countries with robust credit reporting regimes, use of such data has largely been confined to marketing and other related purposes.

This is beginning to change with apps such as www.lenddo.com and www.eflglobal.com, which are using certain kinds of non-financial personal data in FCRA-covered transactions. Whether or not the use of such data succeeds in the long run is difficult to tell, and will ultimately depend on their demonstrated value to lenders, consumers, and the broader society. However, whenever non-financial data are used for credit decisions, both the user and data provider will be subject to the same legal and regulatory requirements that govern the distribution and use of credit reports, including the FCRA, the ECOA, the GBLA, the Fair Housing Act, and other applicable laws. It is not always clear that large scale data aggregators understand the issues involved or the legal requirements associated with the use of their data. For example, Facebook's recent use of its data to block housing advertisements to consumers living in certain zip codes or with certain interests (e.g., support dogs, Latin America, child care providers, etc.) has been cited by HUD as a violation of fair lending laws.[77] While Facebook disputes these charges, it illustrates the dangers inherent in proceeding into largely unchartered territories with inadequate knowledge or regulatory guidance on the applicable rules of the road.

More generally, even if a particular kind of data prove to be highly predictive, there are a number of considerations that may ultimately limit or prevent its actual use in FCRA-covered transactions. The question becomes less a matter of "Can we do it?" but rather, "Should we?" Much like the issue of racial or geographic profiling, the issue of whether such data are predictive is ultimately less important than other overriding economic, social, or ethical concerns. For example, use of certain kinds of data—such as a consumer's Facebook friends or shopping patterns—could have a disparate impact on minorities and other protective classes even if such prohibited factors are not explicit inputs to the decisioning model. In such instances, the burden falls on the creditor to demonstrate that there is no equally effective alternative to the data that could have been used instead. It has been fifty years since the Fair Housing Act was passed, yet Americans remain highly segregated. This basic reality had led some detractors to argue that the use of social networking data or shopping

---

[76] For a detailed discussion, see Tobias Berg, Valentin Burg, Ana Gombović, and Manju Puri, "On the Rise of the FinTechs—Credit Scoring using Digital Footprints", FDIC Center for Financial Research, FDIC CFR WP 2018-04, July 2018.
https://www.fdic.gov/bank/analytical/cfr/2018/wp2018/cfr-wp2018-04.pdf
[77] Ben Lane. "HUD accuses Facebook of enabling housing discrimination." *Housing Wire*, August 17, 2018.
https://www.housingwire.com/articles/46505-hud-accuses-facebook-of-enabling-housing-discrimination?eid=324620953&bid=2211333

patterns for decisioning purposes will only serve to foster racial and ethnic stereotypes and perpetuate discrimination.

It may also be more difficult to verify the accuracy of certain kinds of non-financial personal data, or to explain the results to the consumer if use of such data leads to a credit denial—requirements that are necessary to be FCRA-compliant. For example, frequent bar attendance may well be a statistical predictor of loan performance, but what if the particular consumer claims that she never drinks? And how does a potential creditor tell a consumer that she was turned down for a loan because her educational background, cell phone use, or Facebook interests are generally associated with a higher credit risk? Any statistical scoring model is based on the *average* performance of consumers with similar characteristics. But it is one thing to base a credit decision on financial considerations—for example, a consumer's demonstrated handling of credit—and quite another to base it on the average behavior of groups with similar interests, habits, or "likes." This is the same basic problem, on a macro scale, that led to regulation of CRAs to begin with, namely, using data such as reputation, ethnicity, or gender to assess a consumer's creditworthiness.

Because of such concerns, some creditors may simply be unwilling to use certain types of personal data in order to protect their corporate image and their resulting customer base, even if that data is both predictive and readily verifiable. For example, as one study points out, while consumers' ability to make good on their financial obligations is clearly affected by local economic conditions, geographic region is rarely, if ever part of the credit scoring models most lenders use.[78] According to the authors, "this is most likely due to a concern that the inclusion of such factors could lead to serious public relations problems ... even though there is no legal restriction on the use of such geographic factors in making credit decisions."[79] Indeed, concerns over corporate image may help to explain why Facebook's efforts to develop partnerships with several of the nation's largest banks have thus far been unsuccessful.

Certain kinds of personal data may also be susceptible to manipulation by the consumer, which will ultimately limit its predictive power over time. For example, a consumer's LinkedIn page may well provide information from a consumer's resume (e.g., educational obtainment, job title, etc.) that might initially boost the predictive power of traditional credit scores. But once its use becomes common knowledge, what would stop consumers from altering the information they provide to the website? Likewise, data on the consumer's cell phone use or shopping patterns may in the short term be predictive, but once consumers understand how their data is being used, what's to stop them from changing their habits over time? More generally, in order to be useful for credit decisions, the data should retain its predictive power over various stages of the credit cycle and be resistant to manipulation.

---

[78] Raphael Bostic and Paul Calem, "Privacy Restrictions and the Use of Data at Credit Registries", in *Credit Reporting Systems and the International Economy*, edited by Margaret J. Miller, Boston: MIT Press, 2003, pp. 311-334

[79] Ibid, p. 316

Finally, the voluntary nature of credit reporting may also serve as a barrier to the development and use of certain types of non-financial personal data. FCRA imposes significant requirements on the data furnisher to verify and ensure the accuracy of their data, and to make its use transparent to the consumer. For some large scale data aggregators, this might be a price they are simply unwilling to pay, especially if the use of their data for FCRA-related activities is not an integral part of their overall business strategy. While this may change over time, a general reluctance to take on the full responsibilities of an FCRA-compliant data provider could prove to be a near-term barrier for the use of certain kinds of personal data for credit and other covered purposes.

These considerations suggest that the most promising types of "alternative data' will be those that meet most, if not all, of the criteria presented in Table 3.[80] Financial data that are often part of a manual underwrite (e.g., the timely payment of utility and telecom bills, the consumer's discretionary income) clearly score high on these criteria. However, while non-financial personal data can sometimes serve as a proxy for a consumer's creditworthiness (e.g., time at current residence), use of such data is more likely to be problematic. Under today's legal and regulatory regime, predictive power is not the only factor that will determine whether a specific data element can or should be used in credit decisions. While the underlying values that are embedded in this regime could change over time, in the near term, they may limit the use of certain kinds of personal data in FCRA-covered transactions.

Table 3: Criteria for Assessing the Value of Alternative Data

Criteria	Implications
Compliant	• Compliant with all existing laws and regulations, including the FCRA and ECOA
Predictive Value	• Proven predictive power over various stages of the credit cycle • Not susceptible to manipulation by the consumer • Provides significant value-added over existing credit data
Scope and Coverage	• Available for a significant segment of the population • Available from public sources or voluntarily supplied by data furnishers who are willing to assume the legal and regulatory burdens imposed by existing laws
Accuracy	• Transparent to the consumer • Verifiable by the data furnisher
Social Value	• Use is consistent with broad social and ethical norms and values

A recent Treasury report called for greater regulatory guidance on the use of non-financial personal data in credit decisions in order to remove the uncertainty that might otherwise limit innovation in this area. In particular, it concluded that "regulators should provide regulatory clarity for the use of new data and modeling approaches that are generally recognized as providing predictive value consistent with applicable law for use in credit decisions."[81] The

---

[80] These criteria are largely based on those developed by FICO. See Ann B. Schnare, "Alternative Credit Scores and the Mortgage Market: Opportunities and Limitations," December 2017. Available at www.progressivepolicy.org/publications/updated-credit-scoring-mortgage-market/
[81] US Treasury, op. cit., p.138

report also recommended "prudent experimentation with the aim of working through various issues raised, which may in turn require new approaches to supervision and oversight."[82] These initiatives would certainly be steps in the right direction that would help to reduce the barriers that now exist for the application of certain kinds of non-financial personal data in credit decisions and other FCRA-covered transactions.

4.2 Enhanced Analytics and the Movement to Artificial Intelligence (AI)

Another closely related trend impacting credit bureaus and credit score providers is the development of increasingly sophisticated analytic tools, including machine learning and artificial intelligence (AI). It is difficult to envision how such developments will change the future of credit bureaus, let alone the course of human history. However, in the near term at least, use of advanced analytics for the purposes of granting credit will be subject to basic provisions of the FCRA that are designed to ensure the transparency and equity of credit decisions. In some cases, this could again put limitations on the types of analytics or data that can be used in decisioning models, even at the expense of increased precision.

For example, whenever a credit application is denied, the FCRA requires the creditor to give the consumer a list of the major reasons for their rejection. Yet the algorithms embedded in many advanced decisioning models do not always lend themselves to easy interpretation. While the model's decisions may be sound, the reasons behind those decisions may be opaque and, in some cases, counter-intuitive. As a result, the FCRA's requirement for transparency—which is a key consumer right—may ultimately limit the extent to which enhanced analytics and so-called black-box technologies can be used in the decisioning process. There are solutions to these problems, as evidenced by Equifax's recent use of constrained-neural networks for decisioning models.[83] However, FCRA requirements, along with fair lending laws, will continue to put the burden on both the creditor and the credit score provider to demonstrate that decisioning models are empirically derived, demonstrably and statistically sound, and do not have a disparate impact on protected groups.

Some opponents of AI worry that the growing use of "algorithms" in virtually every aspect of modern life "is changing our approach to accountability from one based on direct causation to one based on correlation, with profound moral and political consequences."[84] To a certain extent, any statistical model is based on correlations, regardless of how it is derived, and any model is only as good as the modeler and the data that are used. While machine learning may avoid the inherent biases that a human modeler might bring and discover previously unknown relationships, it may also lack the underlying value judgement that

---

[82] Ibid. p. 138

[83] Matthew Turner and Michael McBurnett. Optimizing Neural Networks for Risk Assessment. United States Patent US 10,133,980. United States Patent and Trademark Office. November 20, 2018. https://patents.google.com/patent/WO2016160539A1/en

[84] Duncan McCann, Miranda Hall and Robbie Warin, "Controlled By Calculations? Power and Accountability in the Digital Age, Part 3: The Rise of Algorithms," New Economics Foundation, 2018. https://neweconomics.org/uploads/files/Controlled-by-calculations.pdf

reflects broader social and ethical norms. These considerations are especially germane when it comes to credit decisions. It is one thing to assess an individual's creditworthiness based on their past performance on various kinds of financial obligations. It is quite another thing to make a credit decision based on the average performance of other consumers with similar personal characteristics or interests. Not only does this violate the notion of individual accountability; it also raises the specter of "guilt by association."

In the end, the use of advanced decisioning models and alternative data sets, especially in the context of FCRA-covered activities, may well come down to moral and ethical issues related to concepts of "fairness" and "equal access." The ECOA explicitly precludes the use of certain personal characteristics in credit decisions.[85] However, as one study demonstrated with respect to the gender of the borrower, these prohibitions—which the authors characterize as a form of "privacy" restrictions—sometimes come at the cost of model precision. In effect, by imposing these restrictions, "The U.S. Congress decided that the adverse effects of using prohibited bases ... were sufficiently contrary to societal notion of fairness that the potential losses in economic efficiency were justified."[86] Thus, it is entirely conceivable that as the digital economy evolves and its implications are better understood, the list of "protected" classes will expand to preclude the use of other types of personal data in credit decisions, even if such data prove to be highly predictable for certain purposes.

4.3 The Rise of Fintechs and Mobile Payment Apps

Finally, some have argued that the rise of Fintechs and mobile banking apps will undermine the role of credit bureaus and the value of traditional credit reports. One commentator put it this way:

> "Increasingly in a world where payments may involve a peer to peer exchange, a global transfer, and more and more often a mobile phone transaction, the definition of good credit is going to change and widen. The multiple streams of information available about you: where you shop, who your network of friends are, and what you buy may ultimately paint an entirely new, more psychographic way to evaluate your creditworthiness. ... We're about to see more innovative ways of looking at credit, most of them built by mobile-first Fintech companies."[87]

Part of this argument is based on the potential benefits that may arise from introducing new forms of data and analytics into credit decisions. As described in the previous sections, Fintechs operating in this space will be subject to the basic provisions—and potential consequences—established by the FCRA, the ECOA, and other applicable laws. The other part of the argument comes down to whether Fintechs and mobile banking apps will undermine the role of credit bureaus by disintermediating traditional banks—which are the

---

[85] 15 U.S.C. § 1691 et seq.
[86] Bostic and Calem, op. cit., pp. 330-331
[87] Raskin, op. cit.

primary providers and users of credit reports—or by developing new transactions mechanisms (e.g., crypto currencies, peer-to-peer exchanges) that operate outside traditional payment systems, particularly credit cards.

Most mobile payment apps today operate in partnerships with banks, where the bank serves as the intermediary to the transaction by providing access to the consumer's credit card or debit account. The use of such apps could conceivably result in a shift away from credit cards in favor of direct draws from a consumer's bank account, particularly among so-called "transactional" or "convenience" credit card users who pay down their balances every month. If the shift is sufficiently large, it could conceivably reduce the value of credit reports by failing to capture the behavior of such consumers, who represent roughly thirty-nine percent of all active credit card users[88] and are generally better credit risks than those whose balances typically carry over or "revolve." In effect, the current situation would be turned on its head, where consumers with little, if any credit history are actually *better* credit risks than those with more extensive credit files.

However, while one cannot rule out this possibility, there is nothing inherent in these applications that would cause this shift to occur, nor any evidence that such a change is beginning to take place today. Indeed, consumer debt, which declined in the aftermath of the financial crisis, is now at an all-time high of $13.29 trillion,[89] and the percent of adults with revolving credit card balances, while still below pre-crisis levels, has risen in recent years.[90] On the other hand, millennials are in fact less likely to have a credit card than their older counterparts—perhaps portending a long-term shift to debit cards or peer-to-peer exchanges. However, this may simply reflect the fact that this age cohort came out of college with large amounts of student debt at a time when the job market was extremely weak, or the hurdles introduced by The Credit Card Accountability Responsibility and Disclosure (CARD) Act of 2009, which required demonstration of the "ability to pay."

Likewise, Fintechs that operate outside the banking system—for example, lending clubs or crowd-based funders —could conceivably undermine the inherent value of credit reports if such non-banking alternatives captured a significant share of the credit market and were unwilling to share their data. Here, the primary question relates to the voluntary nature of the credit reporting system and whether it will hold up over time. While some Fintechs are currently using the fact that they report to credit bureaus as a marketing tool and to reinforce their customers' incentives to pay on a timely basis, this might not be true for other potential entrants. Reduced reporting raises the risk that a consumer's credit file will become less comprehensive, and therefore less valuable over time. However, given the positive impact that credit reporting has on the borrower's incentives to repay a loan, there is no real reason

---

[88] American Bankers Association, "Credit Conditions Through the Eyes of Consumers, *Credit Card Market Monitor*, July 2018. https://www.aba.com/Press/Documents/2018Q1CreditCardMonitor.pdf

[89] Federal Reserve Bank of New York. *Quarterly Report on Household Debt and Credit: 2018Q2 (August).* https://www.newyorkfed.org/medialibrary/interactives/householdcredit/data/pdf/HHDC_2018Q2.pdf

[90] Jeff Herman, "Credit Card Debt Statistics," *Creditcards.com*, Updated June 6, 2018. https://www.creditcards.com/credit-card-news/credit-card-debt-statistics-1276.php

to suspect that this will actually occur as long as an individual's credit history remains an integral part of lending decisions.

Finally, it is possible that the widespread use of "distributed ledger (DLT)" or "block chain" technology could remove the need for an intermediary between the lender and the consumer by creating a "permanent," "unchangeable" record of a consumer's credit history that the consumer could make available directly to a potential lender. If this in fact occurs, traditional credit reporting agencies could be disintermediated and become a thing of the past, even if a consumer's credit history remains a critical component of lending decisions. However, there are currently significant problems related to the scalability of DLT, as well as to the storing personal data via a technology that depends on thousands of identical copies stored on computers around the globe. While this may change over time, until these problems are solved, the use of such technology is likely to be relatively limited, as least as it relates to the information traditionally provided through credit reports.

A recent Treasury report contained a series of recommendations that could greatly expand the reach of Fintechs by encouraging financial innovation within a regulated space. Among other things, Treasury endorsed the Office of the Comptroller of the Currency's plans to create a new federal bank charter for Fintech firms and called for the creation of a national "sandbox" where firms could seek regulatory guidance before launching a new product or service.[91] If adopted, these recommendations could transform the financial landscape in unknown and inherently unpredictable ways. Stand-alone credit bureaus may well become obsolete as the digital economy evolves. However, as long as there is a need for credit, comprehensive credit reports will likely retain their inherent value and remain part of lending decisions.

5.0 Conclusions and Policy Recommendations

The advent of the digital age, the explosion of personal data and the emergence of artificial intelligence are affecting virtually every aspect of human life, and are raising a series of policy questions ranging from the mundane to the truly profound. One extreme example of how personal data is now being used is China's development of a so-called "social credit score" that could affect virtually every aspect of an individual's life, ranging from the university they attend to their ability to get a job to their access to housing and other social benefits.[92] While U.S. policy makers have begun to address basic questions regarding consumers' control over the collection and use of their personal data, the issues are complex and will inevitably involve trade-offs between the benefits that can result from innovation and the potential costs.

---

[91] U.S. Treasury, op. cit., p. 67, p. 210
[92] Charles Rollet, "The odd reality of life under China's all-seeing credit score system," *Wired*, June 5, 2018. http://www.wired.co.uk/article/china-social-credit

This paper focused on the relatively narrow topic of credit reporting agencies in the digital age. It is too soon to tell how the structure of the industry will change as the digital economy evolves, or the types of data that will ultimately be used as inputs to credit decisions. However, as long as consumers have a need for credit, the functions that credit bureaus currently provide will likely continue to be critical to the well-being of consumers, the efficiency of financial markets, and the strength of the overall economy. In considering broader issues regarding consumer privacy, policymakers need to recognize the unique and important role that credit reporting agencies play. Fortunately, the regulatory and legislative framework that is in place today for credit bureaus can provide the basic guardrails going forward, regardless of the specific data, analytics or platforms that ultimately emerge to support credit decisions.

There is a growing consensus among policymakers and the public that consumers should have the ultimate say over the collection and use of their personal data. However, in the case of credit bureaus, there is a real issue of who actually owns the data—the consumer or the creditor that reports its experience with the consumer? Moreover, even if one believes that the answer is the consumer, "ownership" cannot mean an absolute right to determine the use of credit reports since there are overriding social and economic goals that merit their use even without the consumer's consent. This is why credit information has been, and should continue to be, covered under a special regime—whether via separate laws or distinct chapters in broader data privacy laws—and not lumped in with the broader privacy concerns related to marketing and other uses.

The FCRA's emphasis on restricting the use, rather than the collection of consumer data can also provide a model for addressing other types of privacy concerns. Again, it is tempting to assert that consumers should have the right to "opt in" or "opt out" of various applications of their data. While this may be desirable in theory, it is much more difficult in practice. Consumers rarely take the time to read lengthy disclosure statements, and some applications of consumer data may prove to be so integral to daily living that opting out is simply not a viable solution. Moreover, as is the case for credit reports, some may question whether the service provider, as opposed to the consumer, actually owns the data, for example, when companies such as Google and Facebook provide their services for "free." Finally, and most importantly, there will simply be times when a consumer's desire for privacy conflicts with broader societal goals that might be achieved through their data's use.

In the end, it is difficult to predict how the use of personal data for a variety of innovative purposes will impact the well-being of future generations. For these reasons, many believe that best solution to privacy concerns is to control the use, as opposed to the collection of personal data—the basic approach that was taken by the FCRA. Former Secretary of Homeland Security Michael Chertoff makes this point with respect to national security, concluding that the era of big data "requires both a loosening of what information can be collected by government and at the same time a tightening of the standards under which that

information can be inspected, analyzed, and used."[93] Putting clear restrictions on how various types of consumer data can be used—and ensuring the transparency of the data to consumers—could help to address some of the most egregious misuses of consumer data without unnecessarily stifling innovation. In effect, the FCRA and ECOA can be viewed as a form of privacy restrictions that limit the use of certain personal information in pursuit of the broader public good.[94] While additional characteristics could be added to this list, this general approach is equally applicable to other potential uses of personal data.

Regardless of how the privacy debate is ultimately resolved, policy makers must still address the issue of data security, which is affecting virtually every sector of the economy, including credit bureaus. There are countless examples from both the private and public sectors that illustrate the serious social, economic and national security threats that have arisen from our increasingly digitalized and connected world. Yet slapping large fines on companies that experience a data breach does not prevent breaches from happening, nor does it make the consumer whole. While a patchwork of security laws and regulations are emerging at the state and local levels, broad national security standards have yet to be put in place. In many respects, the current environment is like the Wild West: there are no real rules of engagement, no effective oversight, and no one really in charge.

The above considerations support several broad policy recommendations related to credit bureaus, in particular, and more general issues related to consumer privacy and data security:

➢ First, credit reports are designed to provide an objective and comprehensive view of the consumer's use of credit. As such, concepts such as "opting in" or "opting out" simply do not apply. Policy makers need to recognize this important distinction as they attempt to address broader issues related to consumer privacy, and maintain explicit "carve outs" for credit reporting purposes.

➢ Second, the U.S. legal and regulatory regime that currently governs the use and distribution of credit reports is extremely effective and should be preserved. Further efforts to improve the existing system should focus on consumer education, facilitating access to credit reports, and consumers' ability to redress errors. They should also focus on the kinds of "non-traditional" data that can be—and cannot be—used in FCRA- and ECOA-covered transactions.

➢ Third, policy makers should continue to explore ways to encourage the reporting of telecom, utility and rental payment histories, recognizing that such reporting must include both positive and negative data. While some consumers might see a reduction in their credit score, research has consistently shown that the inclusion of such data would lead to

---

[93] M. Chertoff, *Exploding Data; Reclaiming Our Cyber Security in the Digital Age*, Boston: Atlantic Monthly Press, 2018, p.203.
[94] Bostic and Calem, op. cit., pp. 330-331

a net increase in consumers' access to credit, and that minorities and lower-income consumers would benefit the most.

➢ Fourth, a growing number of Fintechs are beginning to use non-financial personal data as inputs to FCRA-covered transactions. To encourage innovation and avoid "regulation by enforcement"—which benefits no one—policy makers should take steps to develop regulatory guidance on the use of various types of personal data for decisioning purposes. They should also support the creation of so-called "sandboxes" where specific applications can be tested and evaluated without fear of repercussion.

➢ Fifth, when considering more general policies related to the privacy of personal data, policy makers should focus more on the use, as opposed to the collection of such data— the basic approach that was adopted by the FCRA. Uses that are judged to be inconsistent with existing laws or with broader social or ethical values should be explicitly prohibited and if appropriate, incorporated into applicable laws.

➢ Sixth, the Treasury has recently called for uniform national security standards and principles that would pre-empt state and local laws. It is well past time for such an initiative. Such standards should focus on the specific principles and processes that must be put in place to protect a consumer's data and to respond to a data breach, rather than the specific technologies that should be employed.[95] Likewise, any penalties should be based on a company's failure to meet these standards, rather than on the incidence of a data breach.

➢ Finally, absent broad-based Congressional action, there needs to be greater clarity and certainty regarding the specific data security standards that are applicable to credit bureaus, and greater coordination among the relevant regulatory agencies at both the state and federal levels. At a minimum, policy makers should adopt Treasury's recommendation that the relevant regulatory agencies coordinate their actions with respect to the security of credit bureau data, and that Congress assess whether further authorities are needed in this area—including the authority to conduct routine data security compliance reviews. Such actions would go a long way to ensuring that one of the most sensitive kind of personal data—a consumer's credit file—is protected as much as today's technologies will allow.

While admittedly broad in nature, these recommendations will hopefully provide a road map for policy makers as they attempt to address the multitude of complex issues related to credit bureaus, in particular, and to consumer privacy and data security, in general, in an increasingly digitalized world.

---

[95] See for example, National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity" Version 1.1 April 16, 2018.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf