Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Data-Misuse Enforcement Is Focusing On 3 Key Areas

By **David Bitkower, Kali Bracey, Jeremy Creelan, Joseph Noga and Michael Ross**
(July 23, 2019, 2:45 PM EDT)

David Bitkower

Kali Bracey

Jeremy Creelan

Joseph Noga

Michael Ross

Everyone is focused on how companies are using the customer data they collect. Headlines call out changes to privacy rules in Europe, California and elsewhere, and consumers regularly receive notifications of massive data breaches. With all this going on, there is another piece of the data puzzle that companies need to be talking about and preparing for: the wave of enforcement activity that has begun to focus on how companies are using the sensitive data they collect in making business decisions — to approve or deny a loan, to target an advertisement or to pick a neighborhood for offering a new service.

With this wave of activity, and more likely to come, any business that uses sensitive data as part of its decision-making needs to remain focused on more than the rules for how to safeguard sensitive customer data; it must also stay informed about the enforcement actions being taken by regulators throughout the country about how companies use that data to make business decisions. This article addresses three key areas of interest for regulators: discrimination and unfairness, accuracy, and security and transparency.

Data Usage on the Regulator Brain

In recent years, regulators have signaled to the public an increasing concern over the way that companies may be using data about their clients and customers, particularly when it comes to making financial decisions like extending credit. For example, the Federal Trade Commission — which has jurisdiction over consumer protection and competition in commerce — has held multiple hearings over the past several years about the intersection of big data and consumer protection.

Those hearings have focused in part on the concern that using big data in commerce can lead to discrimination and privacy concerns. In 2017, the U.S. Consumer Financial Protection Bureau issued a request for information noting that using alternative, non-FICO data for credit decisions raises regulatory concerns. In 2018, more than 25 state attorneys general submitted comment to the FTC raising consumer welfare concerns regarding use of algorithmic decision tools, artificial intelligence and predictive analytics. These are just a few examples of government authorities becoming more focused on how companies are using the data they collect.

Regulation Through Enforcement

Numerous regulators have authority under existing laws to take action against companies that adversely affect consumers. Most broadly, the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." A practice can be unfair, for example, if it "causes or is likely to cause substantial injury to consumers" that is not outweighed by any countervailing benefits to consumers and that consumers themselves could not reasonably have avoided."

Another provision of federal law enables the CFPB to enforce a prohibition against businesses engaging in "unfair, deceptive, or abusive acts or practices" — the so-called UDAAP authority. And most states have similar provisions that government or private parties can enforce. In short, various existing laws provide broadly worded grants of power to regulators to pursue an enforcement action against consumer-facing activity they deem undesirable. The breadth of the standards, coupled with the variety of enforcement authorities, can make it difficult to predict what practices will fall under regulatory scrutiny.

Discrimination and Unfairness

It is well-established law that companies cannot make business decisions — particularly credit decisions — that discriminate on the basis of a protected characteristic, such as race, gender, religion or country of origin. But what happens when a company employs a decision-making algorithm that does not expressly use race, but uses another factor that ends up serving as a proxy for race? That too can constitute discrimination.

For example the FTC has said that using ZIP code in a decision can be an unlawful proxy for a race-based decision and could therefore constitute an "unfair" practice under the FTC Act. And what about more complex algorithms that use machine learning or nuanced AI to cull data to find correlations that are then used to make decisions on who is credit-worthy and who is not?

For example, crunching available data may show that members of a particular group are more likely to default on loans or apply for less attractive credit products. The FTC has also said that a company could face potential liability for targeting its advertising for only those less attractive products to that group, if it leads to members of the protected group obtaining only those less attractive products. And in its June 28, 2019, fair-lending report, the CFPB noted that "[t]he use of alternative data and modeling techniques may expand access to credit or lower credit cost and, at the same time, present fair lending risks." The agency recommended supervisory reviews of credit-scoring models, and also noted as an area of enforcement focus the use of models to predict recovery outcomes in collecting credit card and auto loan debts.

Two recent examples show how using data analytics to target consumer marketing needs to be approached with particular sensitivity. In one well-publicized example, Amazon.com Inc. failed to offer same-day delivery service to certain minority neighborhoods in New York and other cities. Following claims that Amazon was using geography as proxy for race, a U.S. congressperson sent a letter to the FTC, arguing that Amazon's conduct might be an "unfair" business practice under the FTC Act and violation of the Civil Rights Act of 1964. Amazon quickly expanded its same-day delivery service to those neighborhoods to calm the uproar.

In another example, the U.S. Department of Housing and Urban Development filed a charge of discrimination against Facebook Inc., alleging the company violated the Fair Housing Act "by encouraging, enabling, and causing housing discrimination through the company's advertising platform." Other enforcement actions have focused on the use of data about a customer's source of income (e.g., child support payments) in a credit decision, or targeting loan advertisement to neighborhoods that did not have high numbers of black or Hispanic residents.

As these examples indicate, enforcement authorities will expect companies not to use their data analytics to make decisions that — whether they know it or not — end up targeting or excluding particular consumer groups, or that have a disparate impact on those groups, in a manner that can be considered unfair or discriminatory. Thus, companies ought to be on the look at to ensure they understand the data inputs that are driving decisions; and, as importantly, they need to understand the business reasons they are making decisions, beyond the mere fact that the data has shown a correlation. In other words, just because a data set shows a particular correlation that may not necessarily provide a justification on it own for a decision that could later be challenged.

As a practical matter, it will likely be important for companies to consider including a human element in their assessment process — to look at the input and the outputs, and to look out for correlations that may, even unwittingly, serve as a proxy for a protected characteristic. Critical human input can help guard against employing a process that ends up having unintended, problematic consequences.

Accuracy

Another key, albeit more nascent, area of regulatory concern is the accuracy of alternative data that a company acquires, uses or sells for use in decisions about consumers. After a honeymoon period — where the focus has been the benefits of alternative data with respect to reaching no or thin-file consumers outside the traditional credit system and disrupting the big three credit reporting agencies — consumer advocates and governmental authorities are beginning to question how information is being collected and characterized, and whether it is utilized in a manner consistent with the real-world facts.

The Fair Credit Reporting Act has long provided a framework for assessing the accuracy of traditional consumer credit information. The FCRA provides a basis for consumer reporting agencies to reasonably rely upon sources of information, subject to providing consumers with an opportunity to review and correct the information. It further places certain obligations upon those who furnish information to the reporting agencies and those who obtain information about consumers from them.

By contrast, alternative data is sometimes defined as anything that does not fall within the traditional buckets of information obtained and used by the CRAs. Thus, for those whose operations have a nexus to alternative data, a threshold question is whether they or anyone with whom they are interacting falls within the definition of a CRA and what obligations are imposed if they do. The uninitiated often find the definitions are not intuitive.

Additionally, there is the beginning of a focus on alternative data falling outside the FCRA regulatory scheme. The U.S. Government Accountability Office reported in December 2018 that the CFPB and federal banking regulators are monitoring use of alternative data by collecting information and developing reports, but have not provided specific guidance on using the data. The reliability of data was deemed one of the risks, and the GAO called upon multiple federal agencies to address the appropriate use of alternative data in underwriting.

For its part, the CFPB "commit[ted] to providing information in the future on alternative data" and in the

CFPB's fair-lending report mentioned above stated that a "significant focus" of the Bureau is going to be how credit decisioning models use alternative data. The National Consumer Law Center recently issued a paper that included a warning about errors and inaccuracies in alternative data and the inability to correct them.

Recent FTC enforcement activity has also focused on third-party data. The FTC has settled enforcement cases with data brokers that have failed to give consumers an opportunity to correct erroneous data and for employing dispute resolution procedures that made the correction process particularly burdensome for the consumer. Enforcement has also focused on the failure to provide users of data with notice of when such third-party data was used to adversely affect a credit or other similar decision. Thus, companies selling or using third-party data in relevant consumer decisions should consider whether they have sufficient processes in place to permit user feedback for data, and that they engage in periodic data reviews to assess the completeness or accuracy of their data.

Transparency

The security of consumer data is another key issue for businesses, and keeping up with the rules of numerous government authorities is of paramount importance. But broad enforcement action by consumer protection regulators is also an important aspect of this area to have in mind.

In the leading case of FTC v. Wyndham Worldwide Corporation, the FTC brought an action against the hotel company for failing to adequately safeguard consumer information and for misstating its security practices to those consumers. In that action, the FTC charged that such conduct amounted to unfair or deceptive acts or practices under the FTC Act. Since then the FTC has brought numerous other actions, including against tech companies, under the same basic theory.

Expanding its reach, the FTC has also more recently initiated enforcement actions against tech companies that have not adequately disclosed to consumers the kinds of data they were collecting from them on their platform, as well as other similar theories. As noted above, numerous state regulators have similar authority under parallel state law regimes.

With this area of increasing interest to regulators, it may be expected for regulators using broadly worded enforcement authority to act in still-uncharted areas in which companies are collecting and using various types of sensitive and personal data. Enforcement activity targeting data use that regulators might deem "unfair" could include areas such as facial recognition or automated data collection of repeat, high-volume activities. As these practices become more common, companies should consider conducting periodic audits of data collection and use that involve a cross-section of organizational stakeholders, limiting data collection to what is needed, periodically re-vetting consumer disclosures, and keeping updated with both regulator guidance and enforcement activity.

Conclusion

As data use becomes increasingly key to businesses — and regulators — companies must do more than get up to speed on the basic privacy and data security rules. Enforcement authorities have already laid the groundwork for focusing their attention on whether the ways companies use data can be considered unfair, deceptive or abusive in some way. An existing body of regulatory activity, detailed above, can help guide the way toward the kinds of activities we already know are of interest to government actors — particularly their concern for discrimination, accuracy and transparency. And, as regulators try to keep up with the developments in the way companies are using data, companies are themselves well advised to keep up on enforcement activity by regulators.

David Bitkower, Kali Bracey, Jeremy Creelan, Joseph Noga and Michael Ross are partners at Jenner and Block LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.