Diners, Drive-Ins, and Data Dives: Data Sharing Between Delivery Platforms and Restaurants

Policy Analysis

Restaurant Data Working Group

July 2021

CATALYST RESEARCH

Introduction

Popular third-party food delivery platforms such as DoorDash, Uber Eats, and Grubhub have been "lifelines" for restaurants during the hardest parts of the COVID-19 pandemic, as in-person dining was restricted and people consumed more meals at home. Despite some unhappiness about their fees, the platforms can legitimately say that they provide value, not only in delivery services but also in aggregating diverse restaurant options in one convenient digital location. Consumers and restaurants both utilize delivery services on a strictly voluntary basis, but the system is not at an equilibrium and there is natural tension between the three stakeholders - consumers, restaurants and delivery apps - as the complex food delivery ecosystem continues to evolve.

One point of tension involves the consumer data generated by purchases that delivery platforms analyze to derive insights and optimization strategies. In principle, if individual restaurants had access to such data, analyzing it themselves could help optimize their own operations. However, in practice it is unclear whether the average restaurant is capable of storing, securing, analyzing, and activating this data into meaningful action. Regardless, some policymakers believe that more data sharing with restaurants is a good thing, and to that end the New York City Council is considering legislation (Int. 2311) that would require platforms to share consumer data with restaurants. The latest online summary posted by the City Council reads:

THIS BILL WOULD REQUIRE THIRD-PARTY FOOD DELIVERY SERVICES, ENTITIES THAT PROVIDE FOOD SERVICE ESTABLISHMENTS WITH ONLINE ORDER AND DELIVERY SERVICES, TO SHARE MONTHLY INFORMATION ON CUSTOMERS WHO HAVE PLACED A FOOD OR BEVERAGE ORDER WITH AN ESTABLISHMENT, IF THAT ESTABLISHMENT REQUESTS THE INFORMATION. THE INFORMATION WOULD CONSIST OF THE CUSTOMER'S NAME, PHONE NUMBER, E-MAIL ADDRESS, DELIVERY ADDRESS AND THE CONTENTS OF THEIR ORDERS, AS DESCRIBED IN PROPOSED INT. NO. 2335-A. CUSTOMERS WOULD BE ABLE TO OPT OUT OF THE SHARING OF THIS INFORMATION, AND THE SERVICE WOULD BE REQUIRED TO PROVIDE A CLEAR DISCLOSURE TO CUSTOMERS EXPLAINING WHAT INFORMATION WOULD BE SHARED WITH THE ESTABLISHMENT. THE ESTABLISHMENT FULFILLING THE CUSTOMER'S ORDER WOULD BE PERMITTED TO RETAIN THAT INFORMATION, WHICH MUST BE PROVIDED IN A MACHINE-READABLE FORMAT. SERVICES COULD NOT LIMIT THE ESTABLISHMENTS' USE OF THE INFORMATION, BUT THE BILL WOULD PROHIBIT THE ESTABLISHMENTS FROM SELLING, RENTING OR DISCLOSING THE INFORMATION WITHOUT EXPRESS CONSENT FROM THE CUSTOMER, AND THE CUSTOMER WOULD BE ABLE TO WITHDRAW THEIR CONSENT TO USING THEIR INFORMATION. THE BILL WOULD ALSO PERMIT CUSTOMERS TO REQUEST THAT THE ESTABLISHMENT DELETE THEIR INFORMATION.

While there appears to be some 'guardrails' in the legislation (e.g., prohibiting restaurants from selling the data without express consent), it nevertheless raises several issues worth discussing, as similar policy ideas will undoubtedly be discussed in other cities and states around the

country. The delivery platforms, as well as other experts and thought leaders (e.g., Data Catalyst Institute; Information Technology & Innovation Foundation; Surveillance Technology Oversight Project), have criticized the legislation in its current form.

In order to understand the relevant issues we organized an "expert group" of privacy professionals, law professors, small business advocates, restaurant owners, and industry innovators. The group's insights, in part, drove this initial report on issues related to restaurant data sharing, privacy, and innovation. We plan to conduct follow-on research based on these initial conversations and publish a second report at a later date. Under the Chatham House Rule of non-attribution of information and quotations to encourage candor among participants, we spoke with:

Albert Fox Cahn, Executive Director, Surveillance Technology Oversight Project and Fellow, NYU Law School's Engelberg Center on Innovation Law & Policy

Anupam Chander, Professor of Law, Georgetown University

Ben Ellsworth, Founder & CEO, Gigpro

Emily Hyland, Founder and Partner, Pizza Loves Emily / Emmy Squared Restaurant Group

Jack Collison, Graduate Student, Department of Economics, University of Wisconsin-Madison

Jake Ward, President, Connected Commerce Council

John Breyault, Vice President, Public Policy, Telecommunications, and Fraud, National Consumers League

Jonathan Askin, Professor of Clinical Law and Founding Director, Brooklyn Law and Incubator Policy Clinic, Brooklyn Law School

K Royal, Associate General Counsel and Chief Privacy Officer, TrustArc and Adjunct Professor, Sandra Day O'Connor School of Law, Arizona State University

Mark Bartholomew, Professor of Law, University at Buffalo School of Law

Ryan Calo, Lane Powell and D. Wayne Gittinger Professor, School of Law and Adjunct Professor, Information School and Paul G. Allen School of Computer Science and Engineering, University of Washington

Challenges Associated With Platform-Restaurant Data Sharing

Our conversations with the Expert Group identified a number of challenges associated with the sharing of consumer data between delivery platforms and restaurants. They are: (1) increasing the potential for consumer harm and restaurant liability; (2) assessing the capacity for restaurants to extract value from consumer data; and (3) undermining delivery platforms' business models. We describe these in more detail below.

Increasing the potential for consumer harm and restaurant liability

Regardless of the legislation's specific language, delivery platforms sharing massive amounts of consumer information with restaurants - there are more than 20,000 restaurants in New York City - exposes consumers, restaurants, and platforms to potential liability risks.

Lack of restaurant data security and privacy infrastructure: Although the recently amended legislation now requires restaurants to affirmatively choose to receive data from platforms, many will opt in to receive the data, regardless of their preparedness, in order to experiment with and understand it with the goal of improving their business. By opting in and receiving the data restaurants will immediately assume legal responsibility for data compliance without adequate guidance. Unfortunately, the vast majority of restaurants do not have training or infrastructure to comply with data security and privacy laws, regulations, or best practices, and also may not fully appreciate the risk, potential liability and costs associated with mishandling consumer data.

Unregulated treatment of Personal Identifiable Information (PII): Without expertise in cybersecurity, or a standard set of safety measures in place to prevent misuse or mismanagement of consumer data by restaurants or their employees, restaurant computers could become an unregulated petri dish of people's private information, subject to hacking or other harms, e.g., employee misuse. It is also problematic to combine data received from delivery platforms with internally generated customer data, unless a restaurant has data management technology and training to understand and avoid misuse. These risks are not theoretical:

- Forty-three percent of cyberattacks are aimed at small businesses, but only 14 percent are prepared to defend themselves. (CNBC, 2020)

- Catch Hospitality Group in New York City (Catch NYC, Catch Roof, and Catch Steak) was breached by malware targeting their point-of-service (POS) systems. (TechGenix, 2019 - originally posted on the restaurant group's website but now deleted)

- Large, more sophisticated restaurants are vulnerable, too: Hackers used malware to steal customer payment data from most of Chipotle's restaurants just a few years ago. (Reuters, 2017)

- A more comprehensive list of restaurant data breaches can be found here.

Such data breaches can happen in many ways, ranging from stealing an unsecured laptop or hard drive from a manager's office to sophisticated "phishing" schemes targeting restaurant employees' emails in order to tunnel into a company computer system. Regardless of the exact method, restaurants with a steady flow of fresh customer data will become prime targets for cybercriminals. As a side benefit to the hackers, the legislation conveniently (for hackers) requires the platforms to deliver consumer data in a "machine-readable format."

While data breaches have obviously occurred prior to the introduction of NYC Int. 2311, increased platform-to-restaurant data sharing will make more data available for stealing from more (and less secure) sources. More small restaurants with more consumer data means more "attack vectors" for criminals, with "exponentially more points of failure" for data breaches and abuse. And since restaurants (not platforms) would be the hacker's point of contact for the breach, it is likely they will be sued by consumers and investigated by law enforcement, and face major legal expenses and potentially significant liability. We are assuming, of course, that typical restaurants do not have cyber insurance, which is becoming increasingly expensive due to the recent wave of high-profile and very costly cyberattacks.

We note that this is particularly a threat to minority-owned New York restaurants that, according to the U.S. Black Chamber of Commerce (USBC), are disproportionately harmed by data breaches and cyber attacks. As Ron Busby, USBC President and CEO stated in 2020: "Business continuity and data protection are critical to the success of small companies, as a study we performed with Google confirmed that 98% of black businesses close their doors after being hacked."

Violating reasonable consumer privacy expectations: A massive increase of platform-to-restaurant data sharing as envisioned by NYC Int. 2311 also violates reasonable consumer privacy expectations. First, consumers provide their data to the platforms (which have data security expertise) and not to the restaurants. Notwithstanding the availability of consumer opt-out rights in the amended legislation, consumers will (because the large majority do not read the details of platform privacy policies) be surprised to learn that their data is being shared with restaurants. Beyond their initial surprise, consumers will be aghast to learn that bartenders and just-hired wait staff might have access to their home address, email address, phone number and ordering tendencies. Imagine trying to assign stalking liability when an employee misuses restaurant data to victimize customers. Would liability be assigned to the platform that provided the data, the restaurant that received it, the manager who didn't secure it, or the bartender who peeked at it?

Second, it's unclear to what extent local and national restaurant groups share consumer information internally, far beyond the original NYC location a consumer ordered from. Such internal sharing is generally not considered "disclosing" the data, which the bill prohibits. Third, and perhaps unlawfully, consumers entering New York City from Europe, California and other jurisdictions with stricter privacy protections for their citizens would not expect their data to be shared, and the sharing will likely violate the California Consumer Privacy Act (CCPA) and the EU's General Data Protection Regulation (GDPR).

These issues can result in thought-provoking scenarios that need to be carefully considered. For instance, if a California visitor orders a hamburger through a delivery platform from Shake Shack in Times Square, would a general manager at Shake Shack in West Hollywood, CA have access to the NYC data? Or would a Shake Shack digital marketing manager who likely is trained in California's strict data protection law be able to connect the dots and target this person with very particular ads about being a "jetsetter" - even if California law prohibits this? What is acceptable versus creepy, and who decides?

Legal data sharing between restaurants and third parties: Another way consumer data could flow in legal but unexpected ways would be between restaurants (after they receive it from platforms) and their vendors performing services such as data analysis or digital advertising. Vendors also share data with additional vendors; a "slippery slope" with no end to the number of third parties that could access a consumer's data. This situation may be typical from a business perspective, but it must be carefully regulated when data-sharing is mandatory and further sharing is not tightly constrained with liability clearly assigned.

More than one expert pointed out that these data-resharing and vendor situations make consumers' data more available to non-criminal organizations such as data brokers, hedge funds, and law enforcement, because there are more "access points" to it. It could also indirectly be used in health insurance scenarios (data about a consumers' allergies and food intolerances), divorce cases (data showing that a consumer ordered food to a hotel during work hours), and other sensitive situations.

Unregulated retargeting of customers by restaurants: In its support for NYC Int. 2311, the NYC Hospitality Alliance stated, "This legislation is so important because it removes a major barrier certain third-party delivery companies place between restaurants and their customers, by enabling [the restaurants] ... to directly manage their relationships with their customers, offer them deals, market to them, and more." On the surface, this is reasonable as most restaurants want to build good relationships with their customers. For example, they might ask someone who orders food 1-2 times a month to sign up for their email newsletter or to follow their restaurant on Instagram ("the mecca for hospitality"). And while platform-to-restaurant data sharing would increase the number of potential restaurants targeting frequent food delivery orderers with requests and advertisements, many people already receive so many unwanted emails that this isn't a serious burden or harm.

However, the concern among privacy professionals is that “a few bad apples can spoil the whole bunch.” Because there aren’t well-defined limits on how the restaurants might use the data (besides overtly selling or publishing it), restaurants may do some curious things with it. For example, Major Food Group owns 12 restaurants, including casual Italian restaurant Parm in Nolita and upscale Italian restaurant Carbone in Greenwich Village, which just launched a line of bottled sauces. If I order Spaghetti & Meatballs from Parm once through a delivery app, will I get a marketing email a month later telling me that Carbone Marinara sauce is on sale?

That is a fairly innocent example, but there is nothing stopping a commission-based contract digital marketer from spamming consumers on behalf of restaurant clients that receive troves of customer data from delivery platforms. The legislation also does not limit a restaurant or employee affiliated with a social cause or a political party from targeting consumers with messages about those issues, unrelated to purchasing food.

These concerns do not reflect digital marketing biases against restaurants or any class of business, as we appreciate that delivery platforms also send marketing notifications to customers. However, delivery platform digital marketers are trained in data management practices and legally-required opt-out/unsubscribe options, and informed by data science, careful analysis, experience measuring user behavior, and responsibly “managing their relationships with their customers.”

Assessing the capacity for restaurants to extract value from consumer data

Aside from the data security and privacy issues described above, there is a deeper question that must be asked about platform-to-restaurant data sharing: Does the typical restaurant that would opt-in to receiving this data have the capacity and expertise to extract real value from the data? In other words, would platform-to-restaurant data sharing as described in NYC Int. 2311 provide actual benefit to restaurants, and if so, to which ones exactly, as not all restaurants are the same? Such a benefit would involve transforming the data into insights, which in turn would yield changes to business strategy, operations, and/or tactics.

Restaurant data analysis capacity and expertise: First, we can ask: Does a typical restaurant with slim margins that employs less than 50 people have the capacity and expertise to analyze and operationalize large amounts of consumer data from delivery platform companies? Right now, things are harder than ever for restaurants due to the pandemic (and restrictions and health concerns are not done yet). The National Restaurant Association’s 2021 State of the Restaurant Industry report indicates just how hard the pandemic has hurt the industry:

- As of Dec. 1, 2020, more than 110,000 eating and drinking places were closed for business temporarily, or for good.

- The restaurant industry ended 2020 with total sales that were $240 billion below the Association's pre-pandemic forecast for the year.

- The eating and drinking place sector finished 2020 nearly 2.5 million jobs below its pre-coronavirus level.

While some restaurants are undoubtedly successful because of their brand, specific offerings, or loyal customer bases, many have thought about closing, are experiencing severely reduced revenue, and are understaffed. While deep insights about their customers could in principle help them become more successful, it is unclear how much time and money a typical restaurant would devote to the analysis actually required to find such insights on their own. (Indeed, we believe this would make for an interesting topic of a survey of restaurant owners.)

What would a restaurant owner or senior manager have to do to truly take advantage of a newfound treasure chest of consumer data? Consider a restaurant that gets 50 delivery customers per day, and each customer has 15 associated data points (name, phone, email, etc.). Each month (as required by the legislation) the delivery platform will deliver a data file with 22,500 data points to the restaurant. The restaurant would need to hire a digital marketing data scientist or engage a specialized consultant/vendor. The manager could also take on the task, but whichever way it happens there must be an ongoing commitment of time and/or money. It is entirely possible (or even likely) that a significant number of restaurants initially opt-in to receive large amounts of customer data with well-intentioned plans to use the data to grow the business When the data science/digital marketing challenges quickly become too expensive or complicated, or when the digital marketing consultant angers too many customers by spamming them mercilessly, then the restaurant shuts down its data-driven effort and the customers' data lies permanently dormant in a less-than-secure file folder.

Harm to competition amongst NYC restaurants: Let's assume that some restaurants devote resources to analyzing data and some do not - likely because they are too small and the owners already "wear a million hats." Some decent percentage of the latter group is likely not to opt-in to receiving consumer data from the delivery platforms. While a lack of mandatory sharing and an opt-in for restaurants is good for data security and privacy, the City Council must recognize that it is favoring large restaurants and disfavoring small restaurants by enacting data-sharing legislation that may counterintuitively benefit only the wealthy few.

As a simplified example, imagine that all multiple-location restaurants in NYC opt-in to data sharing and have the capacity and expertise to extract insights from the data. Single-location restaurants do not participate in consumer data sharing. Over time, we would expect the multi-location restaurants to gain an information advantage over single-location restaurants and benefit from investments in targeted digital marketing. The result would be a government benefit bestowed on larger, wealthier restaurants at the expense of smaller restaurants.

It is also notable that chain restaurants such as McDonald's and Chick-fil-A use these same delivery platforms, and the chains typically have sophisticated teams of data scientists and marketers who help optimize operations. We expect these chains would opt-in to receive platform data and make better use the data than most other NYC restaurants. Is this the intention of the sponsors of NYC Int. 2311? As one of our NYC-based experts said: the platform data will help large restaurants further optimize their operations and offerings, but the neighborhood pizza place probably won't benefit at all.

Of course much of this discussion is simply an informed hypothesis, but the potential consequences of favoring large and wealthy restaurants arguably warrants a detailed economic analysis before the Council delivers this extraordinary legislative gift.

Undermining the business models of delivery platforms

Finally, NYC Int. 2311 in effect would undermine the business models at the heart of what allows delivery platform companies to do what they do well in the first place - efficiently facilitate commerce between restaurants and consumers over a distance. Food delivery platform companies derive proprietary insights from the market- and even national-level data they gather, store, analyze, and incorporate into strategies, operations, and tactics. Reducing the proprietary nature of it, and/or forcing it to be shared with third parties who, in effect, directly or indirectly compete with them in an information war, undermines the very business models of these companies. While this may sound ridiculous (how could a restaurant compete against the platform companies?), if every steakhouse in the U.S. banded together into some kind of steak delivery intelligence-sharing cooperative, that could be significant. Delivery platforms have spent millions of dollars in product development and marketing, and forced sharing of valuable consumer data may result in increased fees and/or changes to their business models, which in turn may end up hurting the smallest restaurants that can afford it the least.

It is worth noting that, despite their size, food delivery companies are not (yet) profitable, mainly because transporting food between restaurants and consumers is a complicated and expensive process which literally has to be optimized down to the penny or second. Over the longer term, this data-sharing dynamic with restaurants could lead to less market expansion by platforms, less investment in individual markets, more industry consolidation (i.e., mergers and acquisitions), or even outright failure of some of these companies - all of which, in turn, could actually hurt the restaurants themselves, if every entity in the system is sub-optimized.

"Food is the biggest culture-driver in the world," as one expert noted, and it is worth considering that what many consumers like most about small local neighborhood restaurants is specifically that they are not data-driven and hyper-optimized, replacing human connection with push notifications. Local community restaurants are not commodities and not easily replaceable

specifically because of this - but there is an alternative future world in which every NYC pizza place, food truck, and hipster cafe is optimized for margins, offering you the same deals at the same time at the precisely calculated price and time of day. For some people, that's not a city they want to live in.

Conclusions

Consumer data collected by food delivery platforms - when analyzed safely and insightfully - is a valuable commodity that leads to optimization and better services over time. While restaurants currently do see some of this data (e.g., customer name, phone number, order details), some politicians and regulators believe that food delivery service platforms should be mandated to share more consumer data with restaurants in order to "level the playing field" for small businesses.

While on the surface this may seem like a simple and good idea, there are also a number of challenges with this as currently described in NYC Int. 2311. These challenges include varying degrees of cybersecurity of data by restaurants making them targets for criminals and increasing their legal risk, violating data privacy best practices and creating consumer harm, and unintentionally creating a Darwinian market situation where larger restaurant companies will have the resources to make use of the data from delivery platforms but smaller restaurants will not.

That said, most everyone agrees that more data sharing, if done correctly, could "lift all boats" and be valuable for the restaurant industry as a whole. The topic of solutions is not the focus of this report, but some ideas include minimum cybersecurity standards for consumer data, formal data privacy training for restaurant owners and staff, cyber-insurance requirements for data recipients, delivery platform-provided customer data analysis and insights as a premium offering, platforms and restaurants working together to bridge the insights gap across the delivery and dine-in spaces as consumers return to restaurants in-person, and restaurant customer data infrastructure-as-a-service - in which restaurant data and analyses would be stored and secured by a delivery platform company and could be accessed by authorized restaurant staff through a secure login.

About Catalyst Research

Data Changes Everything.

Catalyst Research solves problems from a different perspective. The intersection of technology, public policy and market trends today will define every aspect of society for the next century. It is against this backdrop that Catalyst Research seeks to better understand, elevate and mobilize the data that allows leaders to think creatively and advocate successfully for a sustainable, safer and more equitable future enabled by technology.

Our firm is organized around critically important practice areas including:

- The Digital Safety Net and Small Businesses
- Digital Innovation as a Threat and Opportunity
- The Microeconomics of the Digital Economy
- Digitally Driven National Competitiveness

We are not generalists, and we come with a formed opinion on these matters. At Catalyst Research, we believe that these topics should be commonly understood and easily accessible to leaders and those in a position to shape society's future.

To do this, we bring together the sharp and deeply sourced experts from across a wide array of topic areas and perspectives, enabling the Catalyst Research team to create engaging conversations, unique insights and relatable stories and publications which can be found on www.catalystresearch.com and our sister organization the Data Catalyst Institute www.datacatalyst.org.