The Data Catalyst Institute (DCI) works to support stakeholders and policymakers as they undertake the important and difficult work of enacting sound, operational public policy governing the use of data by and for consumers and data-focused enterprises. To celebrate good policy and identify challenges of many proposals, DCI considers and reports on regulatory and legislative proposals. (DCI has released a series of detailed 'Report Cards' on policy legislation in the U.S., EU, and other jurisdictions.)

Proposals often evolve — before and even after enactment. To reflect those changes, DCI will monitor amendments, court cases, and other changes in order to adjust our analyses and conclusions. Our objective is not to criticize or condemn, but rather to support better, broader understanding among policymakers, the media, and stakeholders in general.

New York City Council Proposed (Int. 2311)
Data on orders placed through third-party food delivery services

The New York City Council is considering unprecedented data-sharing legislation (Int. 2311) that would force third-party delivery platforms to automatically turn over all customer data to all restaurants from which the customers have ordered food.

The stated purpose of this legislation is to help restaurants communicate directly with customers to ensure high-quality service and provide opportunities for direct marketing by the restaurant to the consumer. The Council understandably wishes to help restaurants that have struggled through the COVID-19 pandemic, but this proposal:

- Is contrary to every government, law enforcement and consumer advocate's stated goals regarding personal privacy, data protection and safety.
- Offers data-collection opportunities to thousands of restaurants that are likely to be unprepared to secure and professionally manage consumer personal data, which is why they choose to work with food delivery platforms. The restaurants have the option of declining data, but the temptation of consumer marketing data will be difficult to resist.
- Opens unprepared restaurants to potential liability, including class action lawsuits and costly fines.
- Makes restaurants into favorable targets as hackers planning their next phishing scheme are always looking for up-to-date consumer data safeguarded by untrained employees.
- Requires food delivery apps to share consumer data with unprepared restaurants, without indemnifying delivery apps to protect them against consumer lawsuits that are inevitable against both the restaurants and the delivery apps.

In the interest of urgency as this bill is moving quickly through the NYC Council, DCI has outlined the challenges of the legislation. Specifically:

Financial and Legal Risks to Restaurants and Consumers Due to Data Breaches

Int. 2311 does not require restaurants receiving consumer data to be certified or have any training regarding protecting and managing consumer data. The unfortunate reality is that most restaurants are not prepared to secure data or utilize "best data management practices," and this will inevitably result in data being exposed; hackers accessing treasure troves of consumer data, and restaurants being sued and fined when mistakes are made and revealed.

- Restaurant Owners Beware: Data Breaches Hurt The Bottom Line - "If your restaurant experiences a data breach, you are likely to have a business interruption, incur fees, fines and costs, suffer reputational damage, and be exposed to enforcement actions by government agencies and potential lawsuits." (Total Food Service, 2019)
- Forty-three percent of cyberattacks are aimed at small businesses, but only 14 percent are prepared to defend themselves (CNBC, 2020)
- Average cost of a cyberattack on a business was $200,000 (Hiscox Cyber Readiness Report of 2019)
- Sixty percent of companies go out of business within six months after falling victim to a data breach (National Security Alliance, 2015)
- A Centrify study found 65 percent of data breach victims lost trust in an organization following a breach (Restaurant Dive, Oct. 2019, citing IBM and Centrify)

Unsecure PII is inevitable and will be harmful to consumers, restaurants, delivery services, and the data-driven industry as a whole.

- Local Restaurants Hit By Data Breach, Customer Info Hacked - "The parent company of several restaurant chains with outlets in the Tri-State Area have been hit by a data breach. Earl Enterprises says a 10-month hack may have exposed credit and debit card information of diners. Restaurants include Buca di Beppo, Planet Hollywood and Earl of Sandwich. **Orders paid online, using third-party platforms, were not part of the breach." (**CBS New York, 2019)
- Chipotle says hackers hit most restaurants in data breach (Reuters, 2017)
- POS Data Breaches: A Comprehensive List of Compromised Restaurants - "According to the latest IBM data breach report, the global average cost of a data breach is $3.26 million—up 6.4 percent from 2017. Point-of-sale data breaches are a serious concern for businesses that can lead to a lack of trust from consumers and a crippled system that could cost a fortune to fix." (Upserve, 2020)
- Upscale New York City Restaurants Experience Data Breach - "New York-based restaurant operator Catch Hospitality Group has been breached by malware targeting their

point-of-service (POS) systems. The affected restaurants are Catch NYC, Catch Roof, and Catch Steak and, as the security alert states, the malware breached the restaurants at different points." (TechGenix, 2019)

Violation of Consumer Expectations

Int. 2311 places the marketing interests of restaurants ahead of the privacy interests of their customers. Int. 2311 does not permit consumers to opt-out of data sharing generally and permanently, but instead requires customers to opt out each and every time they place an order. This decision illustrates sponsors' and supporters' expectation that customers may initially opt out, but inevitably they will forget to opt out and then the restaurants will collect a treasure trove of data.

The first rule of data protection and privacy is respect - for the consumer and the data. Requiring delivery apps to amend their privacy policies that consumers rely on harms both the delivery apps and consumers. There is an expectation among consumers that first-party data collection, e.g., by the app, is legitimate and expected, but that data sharing requires explicit approval and consideration. The City Council choosing to override consumer interests is surprising and contrary, and will irreparably harm consumers' trust in the industry.

Personal safety concerns and child endangerment

By exposing consumer data to untrained and unprepared restaurants, Int. 2311 guarantees that consumer data will be accessible to employees, their friends and associates, and that this will lead to stalking and other personal safety risks. Email addresses, phone numbers, street addresses and credit card numbers could all be stored unprofessionally and insecurely, which is simply dangerous and would be a direct result of a broadly-drafted and not-well-considered government mandate.

Violation of Existing Contracts and Partnerships

Int. 2311 may force businesses to violate existing contracts, and those contracts may incorporate obligations associated with broader laws and policies. For example, college food and retail services rely on delivery platforms and are required to comply with federal education privacy laws (e.g., FERPA). Int. 2311 does not provide an exemption to protect student information, so the result may be that the delivery apps stop working with colleges, or the colleges and apps will choose between violating FERPA or violating Int. 2311.

Burden on consumers to opt-out of EVERY order if they do not want their data shared

"Notification fatigue" occurs when consumers tire of checking the opt-out box repeatedly so they simply ignore the privacy policies and allow all defaults to prevail. This is inevitably what will happen if consumer opt-out is the rule instead of opt-in, and it is the reason why nearly every data privacy advocate rejects this approach.

* * * *

Keeping pace with shifting markets and regulating technologies before they do harm is an admirable goal. The Data Catalyst Institute (DCI) supports well-intentioned policymakers continuing to work for their constituencies. Int. 2311 is rooted in good intention, and may have an operational foundation that could benefit consumers and restaurants eventually, but in its current form it hurts everyone and does catastrophic harm to the progress made in recent years to reduce unwanted data sharing and increase data security.

Secondary data markets always pose risks. A forced secondary data market would do untold harm to millions of New Yorkers, thousands of New York restaurants, and ultimately create a precedent for violating privacy policies and contracts that are, in lieu of a national privacy law, the best way to maintain privacy obligations and security requirements.

The Data Catalyst Institute strongly recommends the New York City Council reconsider Int. 2311, and, at a minimum, address the privacy and independent restaurant liability implications before moving forward.